

Dominion KX II

Benutzerhandbuch

Version 2.3

DKX2-v2.3.0-0M-G

Juli 2010

255-62-4023-00

Einhaltung der FCC-Bestimmungen

In Tests wurde festgestellt, dass das Gerät die Grenzwerte für digitale Geräte der Klasse A gemäß Teil 15 der FCC-Bestimmungen einhält. Diese Grenzwerte sollen in kommerziell genutzten Umgebungen einen angemessenen Schutz vor Störungen bieten. Das in diesem Handbuch beschriebene Gerät erzeugt, verbraucht und gibt unter Umständen hochfrequente Strahlung ab und kann bei unsachgemäßer Installation und Verwendung zu Störungen des Rundfunk- und Fernsehempfangs führen. Der Betrieb dieses Geräts in Wohnumgebungen führt unter Umständen zu schädlichen Störungen.

VCCI-Informationen (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Raritan ist nicht verantwortlich für Schäden an diesem Produkt, die durch einen Unfall, ein Missgeschick, durch Missbrauch, Fremdeingriffe am Produkt oder andere Ereignisse entstanden sind, die sich außerhalb der Kontrolle von Raritan befinden oder unter normalen Betriebsbedingungen nicht auftreten.



Inhalt







Anhang B Aktualisieren des LDAP-Schemas 333

Anhang C Wichtige Hinweise 341





Kapitel 1 Einleitung

In diesem Kapitel

Dominion KX II-Hilfe

Die Dominion KX II-Hilfe enthält Informationen zur Installation, Einrichtung und Konfiguration des Dominion KX II. Sie enthält ebenfalls Informationen zum Zugriff auf Zielserver und Powerstrips, zur Verwendung von virtuellen Medien, zur Verwaltung von Benutzern und Sicherheit sowie zur Wartung und Diagnose von Problemen des Dominion KX II.

Eine PDF-Version des Hilfedokuments kann von der ***Firmware- und Dokumentationsseite von Raritan http://www.raritan.com/support/firmware-and-documentation/*** auf der Raritan-Website heruntergeladen werden. Besuchen Sie die Raritan-Website, um die jeweils neuesten Benutzerhandbücher einzusehen.

Um die Online-Hilfe zu verwenden, muss die Option "Active Content" (Aktive Inhalte) Ihres Browsers aktiviert sein. Wenn Sie den Internet Explorer 7 verwenden, müssen Sie "Scriptlets" aktivieren. Informationen zur Aktivierung dieser Funktionen finden Sie in der Hilfe Ihres Browsers.

Verwandte Dokumentation

Zur Dominion KX II-Hilfe gehört auch eine Dominion KX II-Kurzanleitung für das Gerät sowie eine Dominion KX II VMWare-Kurzanleitung, die Sie auf der ***Firmware- und Dokumentationsseite von Raritan http://www.raritan.com/support/firmware-and-documentation/*** auf der Raritan-Website finden.Installationsanforderungen und -anweisungen für Client-Anwendungen, die mit <ProductName< verwendet werden, finden Sie im Benutzerhandbuch **KVM and Serial Access Clients Guide**, welches ebenso auf der Raritan-Website verfügbar ist. Spezifische Client-Funktionen, die mit Dominion KX II verwendet werden, finden Sie in der Hilfe.

Neuerungen im Hilfedokument

Die folgenden Informationen wurden als Folge von Verbesserungen und Änderung am Gerät und/oder an der Benutzerdokumentation hinzugefügt.

- Sie können nun eine Schichtkonfiguration verwenden, in der ein Dominion KX II-Basisgerät für den Zugriff auf mehrere andere Schichtgeräte verwendet wird. Weitere Informationen zu Schichten finden Sie unter ***Konfigurieren und Aktivieren von Schichten*** (auf Seite 167).
- Nun können Sie von Dominion KX II verwendete HTTP- und/oder HTTPS-Ports konfigurieren. Siehe ***HTTP- und HTTPS-Porteinstellungen*** (auf Seite 165).
- Die neue Sicherheitsmeldungsfunktion ermöglicht Ihnen, eine Sicherheitsmeldung zu erstellen und anzuzeigen sowie Benutzer aufzufordern, eine Sicherheitsvereinbarung während des Anmeldeprozesses von Dominion KX II zu akzeptieren oder abzulehnen. Siehe ***Sicherheitsmeldung*** (auf Seite 249).
- Dominion KX II unterstützt die P2CIM-APS2DUAL- und P2CIM-AUSBDUAL-CIMs, die zwei RJ45-Verbindungen zu unterschiedlichen KVM-Switches enthalten. Siehe ***Unterstützte Paragon-CIMS und Konfigurationen*** (auf Seite 315).
- Die Seite "Port Access" (Portzugriff) enthält eine neue Registerkarte, auf der Sie einen Server basierend auf dem Namen suchen können. Siehe ***Seite "Port Access" (Portzugriff)*** (auf Seite 50).
- Die Hilfe über die Verwendung des AKC enthält zusätzliche Informationen zu den Voraussetzungen. Siehe ***Voraussetzungen für die Verwendung des AKC*** (auf Seite 99).
- Nun können Sie ein aktives USB-Profil von der lokalen Konsole auswählen. Siehe ***USB-Profiloptionen der lokalen Konsole*** (auf Seite 289).

Weitere Erklärungen zu den Änderungen dieser Version des Hilfedokuments finden Sie in den Versionshinweisen.



Überblick über Dominion KX II

Dominion KX II ist ein sicherer digitaler KVM-Switch (Tastatur, Video, Maus) der Unternehmensklasse, der den Zugriff auf BIOS-Ebene (und höher) sowie die Steuerung von Servern über einen Webbrowser von jedem erdenklichen Ort aus ermöglicht. Mit der Standardversion von Dominion KX II können bis zu 64 Server gesteuert werden. Mit dem Dominion KX II-Modell für acht Benutzer können bis zu 32 Server mit dem KX2-832 und bis zu 64 Server mit dem KX2-864 gesteuert werden.

Dominion KX II unterstützt bis zu acht Videokanäle und ermöglicht bis zu acht Benutzern den gleichzeitigen Zugriff auf acht unterschiedliche Videoziele zu einem beliebigen Zeitpunkt. Am Serverschrank ermöglicht Dominion KX II die Steuerung auf BIOS-Ebene von bis zu 64 Servern und anderen IT-Geräten über nur eine Tastatur, einen Monitor und eine Maus. Die integrierten Remotezugriffsfunktionen des Dominion KX II bieten weltweit über einen Webbrowser die gleichen Steuerungsmöglichkeiten.

Dominion KX II lässt sich mittels einer standardmäßigen UTP-Verkabelung (Kategorie 5/5e/6) einfach installieren. Zu seinen erweiterten Funktionen zählen virtuelle Medien, die 128-Bit-Verschlüsselung, zwei Netzteile, die Remote-Stromzufuhrsteuerung, die Integration von Dual-Ethernet, LDAP, RADIUS, Active Directory® und Syslog, externe Modemfunktionen sowie die Webverwaltung. Das Dominion KX II-Modell für acht Benutzer bietet zudem einen erweiterten lokalen Port an der Geräterückseite. Diese Features ermöglichen Ihnen längere Betriebszeiten, eine höhere Produktivität und maximale Sicherheit – jederzeit und an jedem Ort.

Die Dominion KX II-Produkte können als eigenständige Geräte eingesetzt werden und benötigen kein zentrales Verwaltungsgerät. Für größere Rechenzentren und Unternehmen können mithilfe der Verwaltungseinheit CommandCenter Secure Gateway (CC-SG) von Raritan zahlreiche Dominion KX II-Geräte zu einer einzelnen logischen Lösung integriert werden (zusammen mit Dominion SX-Geräten für den seriellen Remotekonsolenzugriff und Dominion KSX-Einheiten für die Remote-/Zweigniederlassungsverwaltung).

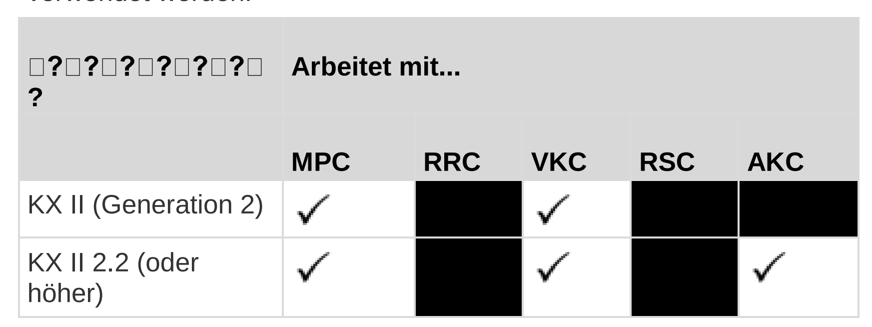



Raritan.

Diagrammschlüssel			
1	Kabel der Kategorie 5	7	Remote-USB-Laufwerk(e) für virtuelle Medien
2	Computer Interface Module (CIM)	8	Powerstrips
3	Dominion KX II	9	Lokaler Zugriff *Hinweis: Die Modelle KX2-832 und KX2-864 nutzen zudem einen erweiterten lokalen Port.*
4	Remote-KVM und serielle Remotegeräte	A	IP LAN/WAN
5	Modem	B	PSTN
6	Remotezugriff (Netzwerk)		

Client-Anwendungen, die mit Dominion KX II verwendet werden können.

Die folgenden Client-Anwendungen können mit Dominion KX II verwendet werden:



□?□?□?□?□?□?□ ?	Arbeitet mit...				
	MPC	RRC	VKC	RSC	AKC
KX II (Generation 2)	✓		✓		
KX II 2.2 (oder höher)	✓		✓		✓

Weitere Informationen zu den Client-Anwendungen finden Sie im Benutzerhandbuch **KVM and Serial Client Guide**. Darüber hinaus finden Sie im Abschnitt ***Arbeiten mit Zielservern*** (auf Seite 43) dieses Handbuchs Informationen zur Verwendung von Clients zusammen mit Dominion KX II.

Hinweis: MPC und VKC benötigen Java™ Runtime Environment (JRE™). Der AKC ist .NET-basiert.

Virtual Media (Virtuelle Medien)

Alle Dominion KX II-Modelle unterstützen virtuelle Medien. Die Vorteile virtueller Medien – Installieren von Remotelaufwerken/-medien auf dem Zielserver zur Unterstützung der Softwareinstallation und -diagnose – stehen nun bei allen Dominion KX II-Modellen zur Verfügung.

Jeder Dominion KX II verfügt über virtuelle Medien, um Remoteverwaltungsaufgaben mithilfe einer Vielzahl von CD-, DVD-, USB-, internen und Remotelaufwerken und Abbildern zu ermöglichen. Im Vergleich zu anderen Lösungen unterstützt Dominion KX II den virtuellen Medienzugriff auf Festplatten und von einem Remotestandort aus installierte Abbilder für mehr Flexibilität und höhere Produktivität.

Virtuelle Mediensitzungen werden durch eine 128-Bit-AES- oder -RC4-Verschlüsselung abgesichert.

Die CIMs (Computer Interface Modules) D2CIM-VUSB und D2CIM-DVUSB unterstützen virtuelle Mediensitzungen mit KVM-Zielservern, die über eine USB 2.0-Schnittstelle verfügen. Diese CIMs unterstützen darüber hinaus den Mausmodus "Absolute Mouse Synchronization™" (Absolute Maussynchronisierung) sowie Remote-Firmwareaktualisierungen.

Hinweis: Der schwarze Anschluss am DVUSB CIM wird zum Anschließen von Maus und Tastatur verwendet. Der graue Anschluss wird für virtuelle Medien verwendet. Achten Sie darauf, dass immer beide Anschlüsse des CIM mit dem Gerät verbunden sind. Es ist möglich, dass das Gerät nicht ordnungsgemäß funktioniert, wenn nicht alle Stecker an den Zielserver angeschlossen sind.



Produktfotos





Dominion KX II



KX2-832



KX2-864





Produktfeatures

Hardware

- Integrierter KVM-über-IP-Remotezugriff
- 1U- oder 2U-Einschub (Halterungen im Lieferumfang enthalten)
- Zwei Netzteile mit Ausfallsicherung; automatischer Wechsel des Netzteils mit Stromausfallwarnung
- 8, 16, 32 oder 64 (beim KX2-464) Serverports
- 32 (KX2-832) oder 64 (KX2-864) Serverports
- Unterstützung für Schichten, in der ein Dominion KX II-Basisgerät für den Zugriff auf mehrere andere Schichtgeräte verwendet wird. Weitere Informationen zu Schichten finden Sie unter ***Konfigurieren und Aktivieren von Schichten*** (auf Seite 167).
- Bis zu acht Videokanäle, je nach Gerätemodell, über die bis zu acht Benutzer gleichzeitig eine Verbindung zu Dominion KX II herstellen können.
- Kapazität für mehrere Benutzer (1/2/4/8 Remotebenutzer, 1 lokaler Benutzer)
- UTP-Serverkabel (Kategorie 5/5e/6)
- Zwei Ethernet-Ports (10/100/1000 LAN) mit Ausfallsicherung
- Während des Betriebs aufrüstbar
- Lokaler Benutzerport für den Serverschrankzugriff
  - Ports für PS/2-Tastatur/Maus Die Modelle KX2-832 und KX2-864 sind reine USB-Geräte.
  - Ein USB 2.0-Port an der Vorderseite und drei an der Rückseite für unterstützte USB-Geräte
  - Simultane Reaktion bei Remotebenutzerzugriff
  - Lokale grafische Benutzeroberfläche (GUI) für die Verwaltung
- Der erweiterte lokale Port bietet erweiterten Serverschrankzugriff auf KX2-Geräte.
- Zentralisierte Zugriffssicherheit
- Integrierte Stromzufuhrsteuerung
- LED-Anzeigen für den Status der beiden Netzteile, Netzwerkaktivität und Remotebenutzerstatus
- Taste zum Zurücksetzen der Hardware
- Serieller Port zur Verbindung mit einem externen Modem

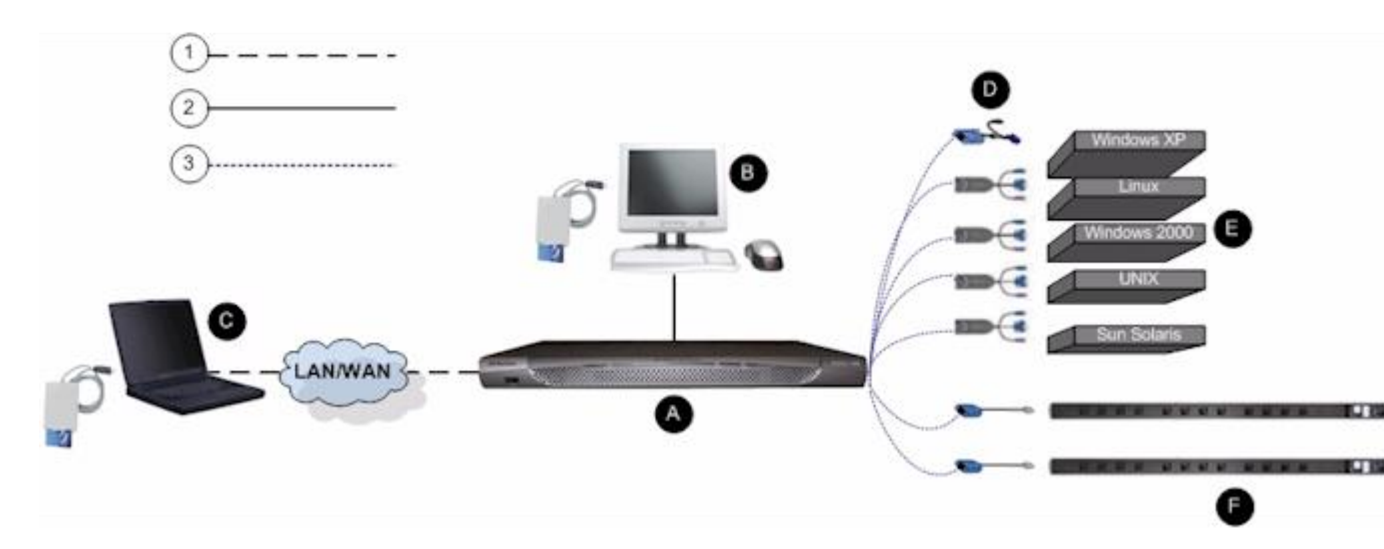
Software

- Virtuelle Medien mit den CIMs D2CIM-VUSB und D2CIM-DVUSB
- "Absolute Mouse Synchronization" (Absolute Maussynchronisierung) mit den CIMs D2CIM-VUSB und D2CIM-DVUSB
- Plug-and-Play
- Webbasierte(r) Zugriff und Verwaltung
- Intuitive grafische Benutzeroberfläche (GUI)
- 128-Bit-Verschlüsselung des gesamten KVM-Signals, einschließlich Video und virtueller Medien
- LDAP-, Active Directory®-, RADIUS- oder interne Authentifizierung und Autorisierung
- DHCP oder feste IP-Adressen
- Smart Card-/CAC-Authentifizierung
- SNMP- und Syslog-Verwaltung
- Unterstützung von IPv4 und IPv6
- Direkt mit Servern verknüpfte Stromzufuhrsteuerung zur Vermeidung von Fehlern
- Integration in die Verwaltungseinheit CommandCenter Secure Gateway (CC-SG) von Raritan
- Feature "CC Unmanage" zum Entfernen eines Geräts aus der CC-SG-Steuerung



Terminologie

In diesem Handbuch wird die im Folgenden erläuterte Terminologie für die Komponenten einer typischen Dominion KX II-Konfiguration verwendet:



Diagrammschlüssel	
1	TCP/IP IPv4 und/oder IPv6
2	KVM (Tastatur, Video, Maus)
3	UTP-Kabel (Kat. 5/5e/6)
A	Dominion KX II
B	Lokale Zugriffskonsole Lokaler Benutzer – eine optionale, direkt mit Dominion KX II verbundene Benutzerkonsole (bestehend aus Tastatur, Maus und MultiSync-VGA-Monitor) für die Steuerung der KVM-Zielserver (direkt am Gestell, nicht über das Netzwerk). Zudem kann ein Smart Card-USB-Lesegerät an den lokalen Port angeschlossen werden, um dieses auf einen Zielserver zu mounten. Die Modelle DKX2-832 und DKX2-864 bieten ebenfalls einen erweiterten lokalen Port.
C	Remote-PC Vernetzte Computer für den Zugriff auf die mit Dominion KX II verbundenen KVM-Zielserver und deren Steuerung. An den Remote-PC kann ebenfalls ein Smart Card-USB-Lesegerät angeschlossen und über Dominion KX II mit einem Zielserver verknüpft werden.
D	CIMs Dongles, die eine Verbindung mit jedem Zielserver oder Powerstrip herstellen. Für alle unterstützten Betriebssysteme verfügbar
E	Zielserver KVM-Zielserver – Server mit Videokarten und Benutzeroberflächen (z. B. Windows®, Linux®, Solaris™ usw.), auf die über Dominion KX II von einem Remotestandort aus zugegriffen wird.
F	Dominion PX-Powerstrips Raritan-Powerstrips, auf die über Dominion KX II von einem Remotestandort aus zugegriffen wird.

Unter ***Unterstützte CIMs und Betriebssysteme (Zielserver)*** (auf Seite 309) finden Sie eine Liste der unterstützten Betriebssysteme und CIMs, und unter ***Unterstützte Betriebssysteme (Clients)*** (auf Seite 319) finden Sie eine Liste der Betriebssysteme, die von Dominion KX II remote unterstützt werden.



Paketinhalt

Jedes Dominion KX II wird als vollständig konfiguriertes, eigenständiges Produkt in einem standardmäßigen 1U-19-Zoll-Gestellchassis (2U für DKX2-864) geliefert. Im Lieferumfang aller Dominion KX II-Geräte ist Folgendes enthalten:

Enthaltene Menge	Element
1	Dominion KX II-Gerät
1	Dominion KX II-Kurzanleitung
1	Gestellmontagekit
1	Netzkabel
1	Netzwerkkabel der Kategorie 5
1	Netzwerk-Crossoverkabel der Kategorie 5
1	Vier Gummifüße (für Schreibtischaufstellung)
1	Anwendungshinweis
1	Garantiekarte

Kapitel 2 Installation und Konfiguration

In diesem Kapitel

Überblick

Dieser Abschnitt enthält einen kurzen Überblick über den Installationsprozess. Die einzelnen Schritte werden im Verlauf des Kapitels noch genauer erläutert.

So installieren und konfigurieren Sie Dominion KX II:

- ***Schritt 1: Konfigurieren von KVM-Zielservern*** (siehe "***Schritt 1: Konfigurieren von KVM-Zielservern***" auf Seite 15)
- ***Schritt 2: Konfigurieren der Einstellungen für die Netzwerkfirewall*** (siehe "***Schritt 2: Konfigurieren der Einstellungen für die Netzwerkfirewall***" auf Seite 29)
- ***Schritt 3: Anschließen der Geräte*** (siehe "***Schritt 3: Anschließen der Geräte***" auf Seite 30)
- ***Schritt 4: Konfigurieren von Dominion KX II*** (siehe "***Schritt 4: Konfigurieren von Dominion KX II***" auf Seite 34)
- ***Schritt 5 (Optional): Konfigurieren der Tastatursprache*** (auf Seite 41)

Dieser Abschnitt enthält außerdem die erforderlichen Informationen zur Standardanmeldung. Dazu zählen die Standard-IP-Adresse, der Standardbenutzername und das Standardkennwort. Siehe ***Standard-Anmeldeinformationen*** (auf Seite 14).

Standard-Anmeldeinformationen

Standard	Wert
Benutzername	Der Standardbenutzername ist "admin". Dieser Benutzer besitzt Administratorrechte.
Kennwort	Das Standardkennwort ist "raritan". Kennwörter unterliegen der Groß-/Kleinschreibung und müssen genau in der bei ihrer Erstellung verwendeten Schreibweise eingegeben werden. Das Standardkennwort "raritan" beispielsweise muss in Kleinbuchstaben eingegeben werden.

Standard	Wert
	Beim ersten Starten des Dominion KX II müssen Sie das Standardkennwort ändern.
IP Address (IP-Adresse)	Dominion KX II wird mit der Standard-IP-Adresse 192.168.0.192 geliefert.

Wichtig: Für die Sicherung und zur Gewährleistung der Geschäftskontinuität sollten Sie unbedingt einen Sicherungs-Benutzernamen und ein Sicherungs-Kennwort für den Administrator erstellen und diese Informationen an einem sicheren Ort aufbewahren.

Erste Schritte

Schritt 1: Konfigurieren von KVM-Zielservern

KVM-Zielserver sind die Computer, auf die über Dominion KX II zugegriffen wird und die von diesem aus gesteuert werden. Konfigurieren Sie vor der Installation des Dominion KX II alle KVM-Zielserver, um eine optimale Leistung sicherzustellen. Diese Konfiguration gilt nur für KVM-Zielserver, nicht jedoch für Clientworkstations (Remote-PCs), die für den Remotezugriff auf Dominion KX II verwendet werden. Weitere Informationen finden Sie unter ***Terminologie*** (auf Seite 11).

Desktop-Hintergrund

Für optimale Bandbreiteneffizienz und Bildleistung müssen KVM-Zielserver mit grafischen Benutzeroberflächen, wie unter Windows®, Linux®, X-Windows, Solaris™ und KDE, konfiguriert werden. Der Desktop-Hintergrund muss nicht völlig einfarbig sein, doch können Hintergrundbilder mit Fotos oder komplexen Farbverläufen die Leistung verringern.

Mauseinstellungen

Dominion KX II arbeitet in verschiedenen Mausmodi:

- Mausmodus "Absolute" (Absolut) ™ (nur D2CIM-VUSB)
- Mausmodus "Intelligent" (verwenden Sie keinen animierten Cursor)
- Mausmodus "Standard"

Für den Mausmodus "Absolute Mouse Synchronization" (Absolute Maussynchronisierung) müssen die Mausparameter nicht geändert werden. Für diesen Modus ist jedoch ein D2CIM-VUSB oder ein D2CIM-DVUSB erforderlich. In den Mausmodi "Standard" und "Intelligent" müssen die Mausparameter auf bestimmte Werte festgelegt werden. Diese Werte werden im Folgenden beschrieben. Mauskonfigurationen können je nach Ziel-Betriebssystem variieren. Weitere Informationen finden Sie in der Dokumentation für Ihr Betriebssystem.

Der Mausmodus "Intelligent" funktioniert auf den meisten Windows-Plattformen. Wenn auf dem Zielgerät der Active Desktop aktiviert ist, kann dieser Modus jedoch zu unvorhersehbaren Ergebnissen führen. Weitere Informationen zu den Einstellungen des Mausmodus "Intelligent" finden Sie unter ***Mausmodus "Intelligent"*** (auf Seite 85).

Server mit internen KVM-Switches innerhalb der Blade-Chassis unterstützen normalerweise keine absolute Maustechnologie.

Einstellungen für Windows 7, Windows XP, Windows 2003 und Windows 2008

► **So konfigurieren Sie KVM-Zielserver, auf denen Microsoft® Windows 7®, Windows XP®, Windows 2003® und Windows 2008® ausgeführt wird:**

1. Konfigurieren der Mauseinstellungen:
   a. Wählen Sie "Start" > "Systemsteuerung" > "Maus" aus.
   b. Klicken Sie auf die Registerkarte "Zeigeroptionen".
   c. Führen Sie im Bereich "Bewegung" folgende Schritte aus:



- Stellen Sie die Mausgeschwindigkeit genau auf die mittlere Geschwindigkeitseinstellung ein.
- Deaktivieren Sie die Option "Enhance pointer precision" (Zeigerbeschleunigung verbessern).
- Deaktivieren Sie die Option "Zur Standardschaltfläche springen".
- Klicken Sie auf OK.

Hinweis: Wenn Sie Windows 2003 auf Ihrem Zielserver ausführen, über KVM auf den Server zugreifen und eine der unten aufgelisteten Aktionen durchführen, kann die Maussynchronisierung deaktiviert werden, wenn diese zuvor aktiviert war. In diesem Fall müssen Sie im Client-Menü "Mouse" (Maus) den Befehl "Synchronize Mouse" (Maus synchronisieren) auswählen, um sie erneut zu aktivieren. Im Folgenden werden die Aktionen aufgelistet, die zur Deaktivierung der Maussynchronisierung führen können:

- Öffnen eines Texteditors

- Zugreifen auf die Maus- oder Tastatureigenschaften sowie Telefon- und Modusoptionen über die Windows-Systemsteuerung.

---

2. Deaktivieren der Übergangseffekte:
   a. Wählen Sie in der Systemsteuerung die Option "Anzeige" aus.
   b. Klicken Sie auf die Registerkarte "Darstellung".
   c. Klicken Sie auf die Schaltfläche "Effekte".
   d. Deaktivieren Sie das Kontrollkästchen "Folgende Übergangseffekte für Menüs und QuickInfos verwenden".
   e. Klicken Sie auf OK.
3. Schließen Sie die Systemsteuerung.

Hinweis: Für KVM-Zielserver, auf denen Windows XP, Windows 2000 oder Windows 2008 ausgeführt wird, können Sie einen Benutzernamen erstellen, der nur für Remoteverbindungen über Dominion KX II verwendet wird. Auf diese Weise können Sie die langsamen Einstellungen für die Mausgeschwindigkeit/-beschleunigung auf die Dominion KX II-Verbindung beschränken.

Die Anmeldeseiten von Windows XP, Windows 2000 und Windows 2008 werden auf die voreingestellten Mausparameter zurückgesetzt. Diese Einstellungen unterscheiden sich von den für eine optimale Leistung von Dominion KX II empfohlenen Einstellungen. Daher ist bei diesen Bildschirmen die Maussynchronisierung möglicherweise nicht optimal.

WARNUNG! Fahren Sie nur fort, wenn Sie sich mit dem Anpassen der Registrierung von Windows-KVM-Zielservern auskennen. Sie können auf den Anmeldeseiten eine bessere Dominion KX II-Maussynchronisierung erzielen, indem Sie hierzu mit dem Registrierungseditor von Windows die folgenden Einstellungen ändern: HKey_USERS\.DEFAULT\Systemsteuerung\Maus: > MouseSpeed = 0;MouseThreshold 1=0;MouseThreshold 2=0.

Einstellungen für Windows 2000

▶ So konfigurieren Sie KVM-Zielserver, auf denen Microsoft® Windows 2000® ausgeführt wird:

1. Konfigurieren der Mauseinstellungen:
   a. Wählen Sie "Start" > "Systemsteuerung" > "Maus" aus.
   b. Öffnen Sie die Registerkarte "Motion" (Bewegung).
      - Stellen Sie die Beschleunigung auf "Keine" ein.
      - Stellen Sie die Mausgeschwindigkeit genau auf die mittlere Geschwindigkeitseinstellung ein.
      - Klicken Sie auf OK.
2. Deaktivieren der Übergangseffekte:
   a. Wählen Sie in der Systemsteuerung die Option "Anzeige" aus.
   b. Klicken Sie auf die Registerkarte "Effekte".
      - Deaktivieren Sie das Kontrollkästchen "Folgende Übergangseffekte für Menüs und QuickInfos verwenden".
3. Klicken Sie auf "OK", und schließen Sie die Systemsteuerung.



Hinweis: Für KVM-Zielserver, auf denen Windows XP, Windows 2000 oder Windows 2008 ausgeführt wird, können Sie einen Benutzernamen erstellen, der nur für Remoteverbindungen über Dominion KX II verwendet wird. Auf diese Weise können Sie die langsamen Einstellungen für die Mausgeschwindigkeit/-beschleunigung auf die Dominion KX II-Verbindung beschränken.

Die Anmeldeseiten von Windows XP, Windows 2000 und Windows 2008 werden auf die voreingestellten Mausparameter zurückgesetzt. Diese Einstellungen unterscheiden sich von den für eine optimale Leistung von Dominion KX II empfohlenen Einstellungen. Daher ist bei diesen Bildschirmen die Maussynchronisierung möglicherweise nicht optimal.

WARNUNG! Fahren Sie nur fort, wenn Sie sich mit dem Anpassen der Registrierung von Windows-KVM-Zielservern auskennen. Sie können auf den Anmeldeseiten eine bessere Dominion KX II-Maussynchronisierung erzielen, indem Sie hierzu mit dem Registrierungseditor von Windows die folgenden Einstellungen ändern: HKey_USERS\.DEFAULT\Systemsteuerung\Maus: > MouseSpeed = 0;MouseThreshold 1=0;MouseThreshold 2=0.

Einstellungen für Windows Vista

- **So konfigurieren Sie KVM-Zielserver, auf denen Windows Vista® ausgeführt wird:**

1. Konfigurieren der Mauseinstellungen:
   a. Wählen Sie "Start" > "Einstellungen" > "Systemsteuerung" > "Maus" aus.
   b. Klicken Sie auf die Registerkarte "Zeigeroptionen".
   c. Führen Sie im Bereich "Bewegung" folgende Schritte aus:
      - Stellen Sie die Mausgeschwindigkeit genau auf die mittlere Geschwindigkeitseinstellung ein.
      - Deaktivieren Sie das Kontrollkästchen "Zeigerbeschleunigung verbessern".
      - Klicken Sie auf OK.
2. Deaktivieren der Animations- und Einblendeffekte:
   a. Wählen Sie in der Systemsteuerung die Option "System".
   b. Wählen Sie "Leistungsinformationen" und anschließend "Tools" > "Weitere Tools" > "Darstellung und Leistung von Windows anpassen" aus.
   c. Klicken Sie auf die Registerkarte "Erweitert".
   d. Klicken Sie in der Gruppe "Performance" (Leistung) auf die Schaltfläche "Settings" (Einstellungen), um das Dialogfeld "Performance Options" (Leistungsoptionen) zu öffnen.

e. Deaktivieren Sie im Bereich "Benutzerdefiniert" die folgenden Kontrollkästchen:

- Animationsoptionen:
  - Steuerelemente und Elemente innerhalb von Fenstern animieren
  - Animation beim Minimieren und Maximieren von Fenstern
- Einblendoptionen:
  - Menüs in Ansicht ein- oder ausblenden
  - QuickInfo in Ansicht ein- oder ausblenden
  - Menüelemente nach Aufruf ausblenden

3. Klicken Sie auf "OK", und schließen Sie die Systemsteuerung.

Einstellungen für Linux (Red Hat 9)

Hinweis: Die folgenden Einstellungen sind nur für den Mausmodus "Standard" optimiert.

▶ So konfigurieren Sie KVM-Zielserver, auf denen Linux® ausgeführt wird (grafische Benutzeroberfläche):

1. Konfigurieren der Mauseinstellungen:
   a. Wählen Sie "Main Menu" > "Preferences" > "Mouse" (Hauptmenü > Einstellungen > Maus) aus. Das Dialogfeld "Mouse Preferences" (Mauseinstellungen) wird angezeigt.
   b. Öffnen Sie die Registerkarte "Motion" (Bewegung).
   c. Stellen Sie in der Gruppe "Speed" (Geschwindigkeit) den Beschleunigungsregler genau auf die mittlere Position ein.
   d. Stellen Sie in der Gruppe "Speed" (Geschwindigkeit) die Sensibilität auf niedrig ein.
   e. Stellen Sie in der Gruppe "Drag & Drop" (Ziehen & Ablegen) den Grenzwert auf niedrig ein.
   f. Schließen Sie das Dialogfeld "Mouse Preferences" (Mauseinstellungen).

Hinweis: Wenn diese Schritte nicht den gewünschten Erfolg erzielen, geben Sie den Befehl "xset mouse 1 1" wie in den Kommandozeilenanweisungen für Linux beschrieben aus.

---

2. Konfigurieren der Bildschirmauflösung:
   a. Wählen Sie "Main Menu" > "System Settings" > "Display" (Hauptmenü > Systemeinstellungen > Anzeige) aus. Das Dialogfeld "Display Settings" (Anzeigeeinstellungen) wird angezeigt.



b. Wählen Sie auf der Registerkarte "Display" (Anzeige) eine Auflösung aus, die von Dominion KX II unterstützt wird.

c. Überprüfen Sie auf der Registerkarte "Advanced" (Erweitert), dass die Aktualisierungsfrequenz von Dominion KX II unterstützt wird.

Hinweis: Wenn eine Verbindung zum Zielserver hergestellt ist, wird bei vielen grafischen Linux-Umgebungen durch den Befehl "<Strg> <Alt> <+>" die Videoauflösung geändert, indem ein Bildlauf durch alle verfügbaren (noch aktivierten) Auflösungen in der Datei "XF86Config" oder "/etc/X11/xorg.conf" (je nach X-Server-Distribution) durchgeführt wird.

▸ So konfigurieren Sie KVM-Zielserver, auf denen Linux ausgeführt wird (Kommandozeile):

1. Stellen Sie die Mausbeschleunigung und den Grenzwert genau auf 1 ein. Geben Sie folgenden Befehl ein: *xset mouse 1 1*. Die Einstellung sollte bei der Anmeldung übernommen werden.
2. Stellen Sie sicher, dass jeder Linux-Zielserver eine von Dominion KX II unterstützte Auflösung mit einer standardmäßigen VESA-Auflösung und Aktualisierungsfrequenz verwendet.
3. Jeder Linux-Zielserver sollte außerdem so eingestellt sein, dass sich die Deaktivierungszeiten im Bereich von ±40 % der VESA-Standardwerte bewegen.
   a. Rufen Sie die Xfree86-Konfigurationsdatei "XF86Config" auf.
   b. Deaktivieren Sie mithilfe eines Texteditors alle nicht von Dominion KX II unterstützten Auflösungen.
   c. Deaktivieren Sie die virtuelle Desktop-Funktion, (nicht von Dominion KX II unterstützt).
   d. Prüfen Sie die Deaktivierungszeiten (±40 % der VESA-Standardwerte).
   e. Starten Sie den Computer neu.



Hinweis: Wenn Sie die Videoauflösung ändern, müssen Sie sich vom Zielserver abmelden und anschließend wieder anmelden, damit die Videoeinstellungen wirksam werden.

Hinweis für Red Hat 9-KVM-Zielserver

Wenn auf dem Zielserver Red Hat® 9 unter Verwendung eines USB-CIM ausgeführt wird und Probleme mit der Tastatur und/oder der Maus auftreten, können Sie eine zusätzliche Konfigurationseinstellung vornehmen.

Tipp: Sie müssen diese Schritte ggf. auch nach der Installation eines Betriebssystems durchführen.

So konfigurieren Sie Red Hat 9-Server mit USB-CIMs:

1. Navigieren Sie zur Konfigurationsdatei Ihres Systems (in der Regel /etc/modules.conf).
2. Verwenden Sie einen Editor Ihrer Wahl und stellen Sie sicher, dass die Zeile "alias usb-controller" in der Datei "modules.conf" wie folgt lautet:

   alias usb-controller usb-uhci

   Hinweis: Wenn die Datei "/etc/modules.conf" bereits eine andere Zeile mit "usb-uhci" enthält, muss die Zeile entfernt oder auskommentiert werden.

   ---

3. Speichern Sie die Datei.
4. Starten Sie das System neu, um die Änderungen zu übernehmen.

Einstellungen für Linux (Red Hat 4)

Hinweis: Die folgenden Einstellungen sind nur für den Mausmodus "Standard" optimiert.

So konfigurieren Sie KVM-Zielserver, auf denen Linux® ausgeführt wird (grafische Benutzeroberfläche):

1. Konfigurieren der Mauseinstellungen:
   a. Wählen Sie "Main Menu" > "Preferences" > "Mouse" (Hauptmenü > Einstellungen > Maus) aus. Das Dialogfeld "Mouse Preferences" (Mauseinstellungen) wird angezeigt.
   b. Öffnen Sie die Registerkarte "Motion" (Bewegung).
   c. Stellen Sie in der Gruppe "Speed" (Geschwindigkeit) den Beschleunigungsregler genau auf die mittlere Position ein.
   d. Stellen Sie in der Gruppe "Speed" (Geschwindigkeit) die Sensibilität auf niedrig ein.



e. Stellen Sie in der Gruppe "Drag & Drop" (Ziehen & Ablegen) den Grenzwert auf niedrig ein.

f. Schließen Sie das Dialogfeld "Mouse Preferences" (Mauseinstellungen).

Hinweis: Wenn diese Schritte nicht den gewünschten Erfolg erzielen, geben Sie den Befehl "xset mouse 1 1" wie in den Kommandozeilenanweisungen für Linux beschrieben aus.

---

2. Konfigurieren der Bildschirmauflösung:

   a. Wählen Sie "Main Menu" > "System Settings" > "Display" (Hauptmenü > Systemeinstellungen > Anzeige) aus. Das Dialogfeld "Display Settings" (Anzeigeeinstellungen) wird angezeigt.

   b. Wählen Sie auf der Registerkarte "Settings" (Einstellungen) eine Auflösung aus, die von Dominion KX II unterstützt wird.

   c. Klicken Sie auf OK.

Hinweis: Wenn eine Verbindung zum Zielserver hergestellt ist, wird bei vielen grafischen Linux-Umgebungen durch den Befehl "<Strg> <Alt> <+>" die Videoauflösung geändert, indem ein Bildlauf durch alle verfügbaren (noch aktivierten) Auflösungen in der Datei "XF86Config" oder "/etc/X11/xorg.conf" (je nach X-Server-Distribution) durchgeführt wird.

Hinweis: Wenn Sie die Videoauflösung ändern, müssen Sie sich vom Zielserver abmelden und anschließend wieder anmelden, damit die Videoeinstellungen wirksam werden.

Einstellungen für SUSE Linux 10.1

Hinweis: Versuchen Sie nicht, die Maus bei der SUSE Linux®-Anmeldeaufforderung zu synchronisieren. Sie müssen mit dem Zielserver verbunden sein, um die Cursor zu synchronisieren.

▸ So konfigurieren Sie die Mauseinstellungen:

1. Wählen Sie "Desktop" > "Control Center" (Desktop > Steuerzentrale) aus. Das Dialogfeld "Desktop Preferences" (Desktopeinstellungen) wird angezeigt.
2. Klicken Sie auf "Mouse" (Maus). Das Dialogfeld "Mouse Preferences" (Mauseinstellungen) wird angezeigt.
3. Öffnen Sie die Registerkarte "Motion" (Bewegung).
4. Stellen Sie in der Gruppe "Speed" (Geschwindigkeit) den Beschleunigungsregler genau auf die mittlere Position ein.
5. Stellen Sie in der Gruppe "Speed" (Geschwindigkeit) den Sensibilitätsregler auf niedrig ein.

6. Stellen Sie in der Gruppe "Drag & Drop" (Ziehen & Ablegen) den Grenzwertregler auf niedrig ein.
7. Klicken Sie auf "Close" (Schließen).

So konfigurieren Sie die Videoeinstellungen:

1. Wählen Sie "Desktop Preferences" > "Graphics Card and Monitor" (Desktopeinstellungen > Grafikkarte und Monitor) aus. Das Dialogfeld "Card and Monitor Properties" (Karten- und Monitoreigenschaften) wird angezeigt.
2. Überprüfen Sie, dass eine Auflösung und eine Aktualisierungsfrequenz verwendet werden, die von Dominion KX II unterstützt werden. Weitere Informationen finden Sie unter ***Unterstützte Videoauflösungen*** (auf Seite 323).

Hinweis: Wenn Sie die Videoauflösung ändern, müssen Sie sich vom Zielserver abmelden und anschließend wieder anmelden, damit die Videoeinstellungen wirksam werden.

Speichern der Linux-Einstellungen

Hinweis: Die Vorgehensweise kann je nach verwendeter Linux®-Version leicht abweichen.

So speichern Sie Ihre Linux-Einstellungen (Aufforderung):

1. Wählen Sie "System Menu" > "Preferences" > "Personal" > "Sessions" (Systemmenü > Einstellungen > Eigene > Sitzungen) aus.
2. Klicken Sie auf die Registerkarte "Session Options" (Sitzungsoptionen).
3. Aktivieren Sie das Kontrollkästchen "Prompt on log off" (Aufforderung bei Abmeldung) und klicken Sie auf OK. Bei dieser Option werden Sie dazu aufgefordert, Ihre aktuelle Sitzung zu speichern, wenn Sie sich abmelden.
4. Wählen Sie bei der Abmeldung im Dialogfeld die Option "Save current setup" (Aktuelle Einstellungen speichern) aus.
5. Klicken Sie auf OK.

Tipp: Wenn Sie nicht bei jeder Abmeldung zum Speichern aufgefordert werden möchten, führen Sie stattdessen die folgenden Schritte durch.

So speichern Sie Ihre Linux-Einstellungen (keine Aufforderung):

1. Wählen Sie "Desktop" > "Control Center" > "System" > "Sessions" (Desktop > Steuerzentrale > System > Sitzungen) aus.
2. Klicken Sie auf die Registerkarte "Session Options" (Sitzungsoptionen).

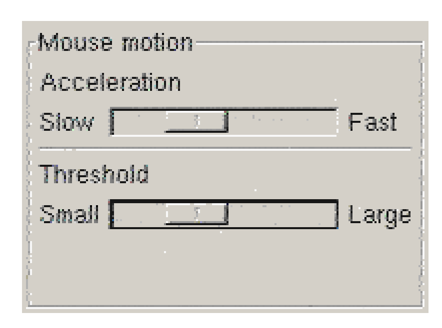


3. Deaktivieren Sie das Kontrollkästchen "Prompt on the log off" (Aufforderung bei Abmeldung).
4. Aktivieren Sie das Kontrollkästchen "Automatically save changes to the session" (Änderungen der Sitzung automatisch speichern) und klicken Sie auf OK. Bei dieser Option wird Ihre aktuelle Sitzung automatisch gespeichert, wenn Sie sich abmelden.

Einstellungen für Sun Solaris

So konfigurieren Sie KVM-Zielserver, auf denen Sun™ Solaris™ ausgeführt wird:

1. Stellen Sie die Mausbeschleunigung und den Grenzwert genau auf 1 ein. Dies kann über folgende Optionen durchgeführt werden:
   - Über die grafische Benutzeroberfläche.



   - Über die Kommandozeile *xset mouse a t*, wobei *a* die Beschleunigung und *t* der Grenzwert ist.
2. Alle KVM-Zielserver müssen mit einer Anzeigeauflösung konfiguriert werden, die von Dominion KX II unterstützt wird. Zu den am häufigsten verwendeten unterstützten Auflösungen für Sun-Systeme zählen:

Anzeigeauflösung	Vertikale Aktualisierungsfrequenz	Seitenverhältnis
1600 x 1200	60 Hz	4:3
1280 x 1024	60, 75, 85 Hz	5:4
1152 x 864	75 Hz	4:3
1024 x 768	60, 70, 75, 85 Hz	4:3
800 x 600	56, 60, 72, 75, 85 Hz	4:3
720 x 400	85 Hz	9:5
640 x 480	60, 72, 75, 85 Hz	4:3

3. KVM-Zielserver mit dem Solaris-Betriebssystem müssen eine VGA-Buchse mit TV-Out-Signal haben (mit H- und V-Synchronisierung, keine Composite-Synchronisierung).

So ändern Sie den Sun-Grafikkartenausgang von der Composite-Synchronisierung auf die nicht standardmäßige VGA-Ausgabe:

1. Geben Sie den Befehl "Stop+A" aus, um in den BootProm-Modus zu wechseln.
2. Geben Sie den folgenden Befehl aus, um die Ausgabeauflösung zu ändern: *setenv output-device screen:r1024x768x70*
3. Starten Sie den Server mit dem Befehl `boot` neu.

Sie können sich stattdessen auch an Ihren Raritan-Ansprechpartner wenden und einen Videoausgabeadapter erwerben.

Vorhandene Einstellung	Zu verwendender Videoausgabeadapter
Sun 13W3 mit Composite-Synchronisierungsausgabe	APSSUN II Guardian-Converter
Sun HD15 mit Composite-Synchronisierungsausgabe	1396C-Converter für die Konvertierung von HD15 zu 13W3 und ein APSSUN II Guardian-Converter, der die Composite-Synchronisierung unterstützt
Sun HD15 mit separater Synchronisierungsausgabe	APKMSUN Guardian-Converter

Hinweis: Einige Sun-Hintergrundanzeigen werden möglicherweise auf bestimmten Sun-Servern mit dunklen Rändern nicht exakt zentriert abgebildet. Verwenden Sie einen anderen Hintergrund, oder platzieren Sie oben in der linken Ecke ein helles Symbol.

Mauseinstellungen

So konfigurieren Sie die Mauseinstellungen (Sun Solaris 10.1):

1. Wählen Sie den Launcher aus. Die "Desktop Controls" (Desktopsteuerung) des "Application Manager" (Anwendungsmanager) wird geöffnet.
2. Wählen Sie "Mouse Style Manager" (Mausstilmanager) aus. Das Dialogfeld "Mouse" (Maus) des "Style Manager" (Stilmanager) wird angezeigt.
3. Stellen Sie den Beschleunigungsregler auf 1.0.
4. Stellen Sie den Grenzwertregler auf 1.0.
5. Klicken Sie auf OK.



Aufrufen der Kommandozeile

1. Klicken Sie auf die rechte Maustaste.
2. Wählen Sie "Tools" > "Terminal" (Tools > Endgerät) aus. Ein Terminalfenster wird angezeigt. (Sie sollten sich auf Stammebene befinden, um Befehle auszugeben.)

Videoeinstellungen (POST)

Sun-Systeme verfügen über zwei verschiedene Auflösungseinstellungen: eine POST- und eine GUI-Auflösung. Führen Sie diese Befehle von der Kommandozeile aus durch.

Hinweis: 1024x768x75 wird hier als Beispiel verwendet. Ersetzen Sie das Beispiel durch die Auflösung und Aktualisierungsfrequenz, die Sie verwenden.

So überprüfen Sie die aktuelle POST-Auflösung:

- Führen Sie den folgenden Befehl als Stammbenutzer aus: `# eeprom output-device`

So ändern Sie die POST-Auflösung:

1. Führen Sie `# eeprom output-device=screen:r1024x768x75` aus.
2. Melden Sie sich ab, oder starten Sie den Computer neu.

Videoeinstellungen (GUI)

Die GUI-Auflösung kann je nach verwendeter Grafikkarte mithilfe unterschiedlicher Befehle überprüft und eingestellt werden. Führen Sie diese Befehle von der Kommandozeile aus durch.

Hinweis: 1024x768x75 wird hier als Beispiel verwendet. Ersetzen Sie das Beispiel durch die Auflösung und Aktualisierungsfrequenz, die Sie verwenden.

Karte	Überprüfen der Auflösung durch:	Ändern der Auflösung durch:
32-Bit	# /usr/sbin/pgxconfig -prconf	1. # /usr/sbin/pgxconfig -res 1024x768x75 2. Melden Sie sich ab, oder starten Sie den Computer neu.
64-Bit	# /usr/sbin/m64config -prconf	1. # /usr/sbin/m64config -res 1024x768x75 2. Melden Sie sich ab, oder starten Sie den Computer neu.
32-Bit und 64-Bit	# /usr/sbin/fbconfig -prconf	1. # /usr/sbin/fbconfig -res 1024x768x75 2. Melden Sie sich ab, oder starten Sie den Computer neu.

Einstellungen für IBM AIX 5.3

Führen Sie die folgenden Schritte durch, um KVM-Zielserver zu konfigurieren, auf denen IBM® AIX™ 5.3 ausgeführt wird.

So konfigurieren Sie die Maus:

1. Öffnen Sie den Launcher.
2. Wählen Sie "Style Manager" (Stilmanager) aus.
3. Klicken Sie auf "Mouse" (Maus). Das Dialogfeld "Mouse" (Maus) des "Style Manager" (Stilmanager) wird angezeigt.
4. Stellen Sie mithilfe der Schieberegler die Mausbeschleunigung und den Grenzwert auf 1.0.
5. Klicken Sie auf OK.

So konfigurieren Sie die Videoeinstellungen:

1. Wählen Sie im Launcher "Application Manager" (Anwendungsmanager) aus.
2. Wählen Sie "System_Admin" aus.
3. Wählen Sie "Smit" > "Devices" > "Graphic Displays" > "Select the Display Resolution and Refresh Rate" (Smit > Geräte > Grafische Anzeigen > Anzeigeauflösung und Aktualisierungsfrequenz auswählen) aus.
4. Wählen Sie die verwendete Grafikkarte aus.



5. Klicken Sie auf "List" (Auflisten). Eine Liste der Anzeigemodi wird angezeigt.
6. Wählen Sie eine Auflösung und Aktualisierungsfrequenz aus, die von Dominion KX II unterstützt wird. Weitere Informationen finden Sie unter ***Unterstützte Videoauflösungen*** (auf Seite 323).

Hinweis: Wenn Sie die Videoauflösung ändern, müssen Sie sich vom Zielserver abmelden und anschließend wieder anmelden, damit die Videoeinstellungen wirksam werden.

Speichern der UNIX-Einstellungen

Hinweis: Diese Vorgehensweise kann je nach UNIX®-Typ (z. B. Solaris™, IBM® AIX™) oder verwendeter Version leicht abweichen.

1. Wählen Sie "Style Manager" > "Startup" (Stilmanager > Start) aus. Das Dialogfeld "Startup" (Start) des Style Manager (Stilmanager) wird angezeigt.
2. Wählen Sie im Dialogfenster "Logout Confirmation" (Abmeldebestätigung) die Option "On" (Ein) aus. Bei dieser Option werden Sie dazu aufgefordert, Ihre aktuelle Sitzung zu speichern, wenn Sie sich abmelden.

Einstellungen für Apple Macintosh

Bei KVM-Zielservern, auf denen ein Apple Macintosh®-Betriebssystem ausgeführt wird, sollten Sie das D2CIM-VUSB und den Mausmodus "Absolute Mouse Synchronization" (Absolute Maussynchronisierung) verwenden.

Hinweis: Das USB-Profil für Mac OS-X Version 10.4.9 und höher muss im Menü "USB Profile" (USB-Profil) oder auf der Seite "Port Configuration" (Portkonfiguration) ausgewählt werden.

Schritt 2: Konfigurieren der Einstellungen für die Netzwerkfirewall

Um über eine Netzwerkfirewall im Multi-Platform-Client oder über die Seite "Port Access" (Portzugriff) auf Dominion KX II zuzugreifen, muss die Firewall die Kommunikation über TCP-Port 5000 oder einen anderen von Ihnen zugewiesenen Port zulassen.

Features des Dominion KX II:	Benötigte Firewalleinstellungen für eingehende Kommunikation
Webzugriffsfunktionen	Port 443 – Standard-TCP-Port für HTTPS-Kommunikation
Automatische Umleitung von HTTP-Anfragen an HTTPS (sodass die bekannteren Adressen	Port 80 – Standard-TCP-Port für HTTP-Kommunikation

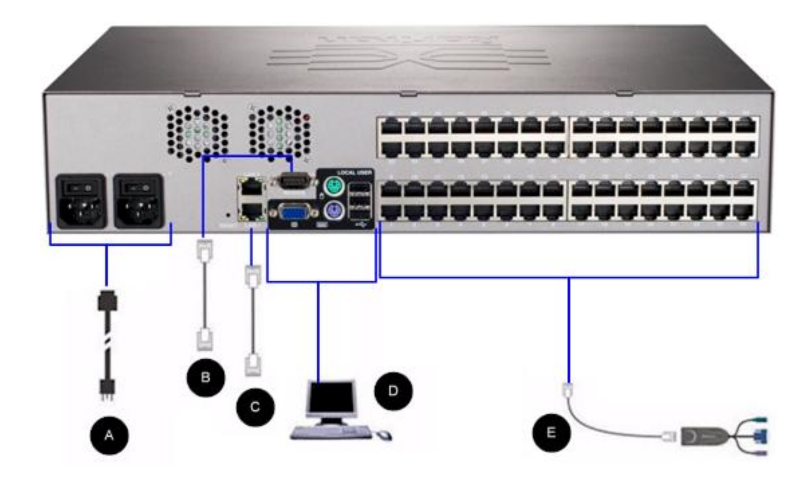


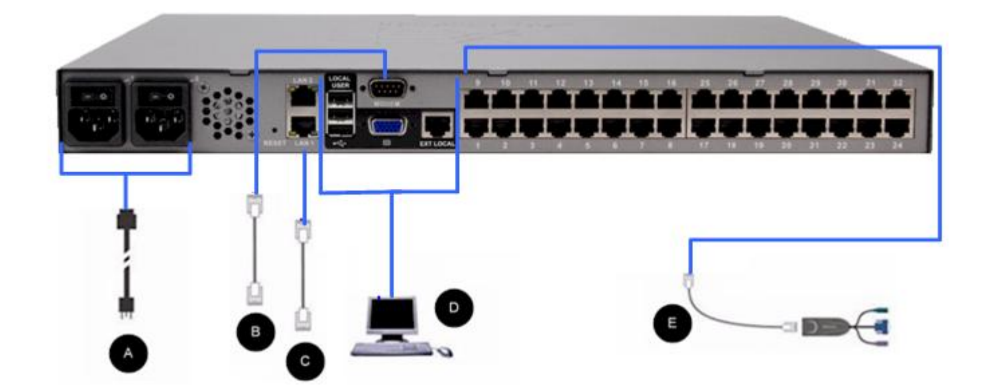
"http://xxx.xxx.xxx.xxx" anstelle von "https://xxx.xxx.xxx.xxx" verwendet werden können)	

Weitere Informationen zum Festlegen eines anderen Erkennungsports finden Sie unter ***Netzwerkeinstellungen*** (auf Seite 157).

Schritt 3: Anschließen der Geräte

Schließen Sie Dominion KX II an die Stromversorgung, das Netzwerk, den lokalen PC und die Zielserver an. Die Buchstaben im Diagramm entsprechen den Themen in diesem Abschnitt, in denen die Verbindung erläutert wird.





A. Wechselstromversorgung

So schließen Sie die Stromversorgung an:

1. Verbinden Sie das beiliegende Netzkabel mit Dominion KX II, und schließen Sie es an die Wechselstromversorgung an.



2. Wenn eine Ausfallsicherung in Form zweier Netzteile gewünscht wird, schließen Sie das zweite beiliegende Netzkabel an, und stecken Sie es an einem anderen Netzteil ein als das erste Netzkabel.

Hinweis: Wenn Sie nur ein Netzkabel mit dem System verbinden, leuchtet die Stromversorgungs-LED-Anzeige auf der Vorderseite des Dominion KX II rot, da das System für die automatische Erkennung beider Stromquellen eingerichtet ist. Informationen zum Deaktivieren der automatischen Erkennung für die nicht genutzte Stromquelle finden Sie unter **Netzteilkonfiguration** *(auf Seite 185).*

B. Modemport (Optional)

Dominion KX II besitzt einen dedizierten Modemport für den Remotezugriff, auch wenn das LAN/WAN nicht verfügbar ist. Verbinden Sie mithilfe eines seriellen (RS-232) Straight-Through-Kabels ein externes serielles Modem mit dem Port mit der Bezeichnung MODEM auf der Rückseite des Dominion KX II (Eine Liste der zertifizierten Modems finden Sie unter ***Spezifikationen*** (siehe "***Technische Daten***" auf Seite 304) und Informationen zur Konfiguration des Modems unter ***Konfigurieren der Modemeinstellungen*** (auf Seite 173)).

Hinweis: Raritan empfiehlt, das Modem durch Aktivieren der Einstellung CD (Carrier Detect) zu konfigurieren.

C. Netzwerkport

Dominion KX II verfügt zur Ausfallsicherung über zwei Ethernet-Ports (dienen nicht zum Lastausgleich). Standardmäßig ist nur LAN1 aktiviert, und das automatische Failover ist deaktiviert. Wenn die interne Netzwerkschnittstelle des Dominion KX II oder der mit diesem verbundene Netzwerkswitch nicht verfügbar sein sollte, wird der Port LAN2 unter Verwendung derselben IP-Adresse aktiviert, sofern das automatische Failover aktiviert wurde.

Hinweis: Da ein Failoverport erst aktiviert wird, wenn tatsächlich ein Ausfall stattgefunden hat, empfiehlt Raritan, den Failoverport nicht zu überwachen oder ihn erst zu überwachen, nachdem ein Ausfall stattgefunden hat.

▶ So stellen Sie eine Netzwerkverbindung her:

1. Verbinden Sie den Netzwerkport LAN1 über ein standardmäßiges Ethernet-Kabel (im Lieferumfang enthalten) mit einem Ethernet-Switch, -Hub oder -Router.
2. Führen Sie die folgenden Schritte aus, wenn Sie die optionalen Ethernet-Failoverfunktionen des Dominion KX II nutzen möchten:

- Verbinden Sie den Netzwerkport LAN2 über ein standardmäßiges Ethernet-Kabel mit einem Ethernet-Switch, -Hub oder -Router.
- Aktivieren Sie auf der Seite "Network Configuration" (Netzwerkkonfiguration) die Option "Automatic Failover" (Automatisches Failover).

Hinweis: Verwenden Sie nur beide Netzwerkports, wenn Sie einen als Failoverport nutzen möchten.

D. Port für den lokalen Zugriff (lokaler PC)

Für den bequemen Zugriff auf Zielserver am Serverschrank kann der Port für den lokalen Zugriff von Dominion KX II verwendet werden. Der Port für den lokalen Zugriff wird für die Installation und Konfiguration benötigt, die weitere Verwendung dieses Ports ist jedoch optional. Der Port für den lokalen Zugriff bietet eine grafische Benutzeroberfläche der lokalen Dominion KX II-Konsole, die für die Verwaltung und für den Zugriff auf Zielserver verwendet wird.

Die Geräte KX2-832 und KX2-864 verfügen für den Zugriff auf Zielserver vom Serverschrank über einen erweiterten lokalen Port, der auf der Geräterückseite mit "EXT LOCAL" gekennzeichnet ist. Der erweiterte lokale Port ist für die erste Installation und Konfiguration nicht erforderlich. Er wird über die lokale und die Remote-Konsole konfiguriert. Weitere Informationen finden Sie unter ***Lokale Porteinstellungen für Dominion KX II konfigurieren*** (auf Seite 225).

So stellen Sie eine Verbindung zum lokalen Port her:

- Schließen Sie einen MultiSync-VGA-Monitor, eine Maus und eine Tastatur an die jeweiligen Ports mit der Bezeichnung "Local User" (Lokaler Benutzer) an. Verwenden Sie eine PS/2- oder USB-Tastatur und -Maus (DKX2-832 und DKX2-864 verfügen nur über USB). Die physischen Anschlüsse für die Ports "Lokal User" (Lokaler Benutzer) und "Extended Local" (Erweitert lokal) finden Sie auf der Rückseite des Dominion KX II-Geräts.

Verbindung	Beschreibung
Monitor	Schließen Sie einen standardmäßigen MultiSync-VGA-Monitor am HD15-Videoport (weiblich) an.
Tastatur	Schließen Sie entweder eine standardmäßige PS/2-Tastatur am Mini-DIN6-Tastaturport (weiblich) oder eine standardmäßige USB-Tastatur an einem der USB Typ A-Ports (weiblich) an.



Maus	Schließen Sie entweder eine standardmäßige PS/2-Maus am Mini-DIN6-Mausport (weiblich) oder eine standardmäßige USB-Maus an einem der USB Typ A-Ports (weiblich) an.

E. Zielserverports

Dominion KX II verwendet standardmäßige UTP-Verkabelung (Kat. 5/5e/6) zur Verbindung mit jedem Zielserver.

So stellen Sie eine Verbindung zwischen einem Zielserver und Dominion KX II her:

1. Verwenden Sie das entsprechende CIM (Computer Interface Module). Informationen zu den mit dem jeweiligen Betriebssystem zu verwendenden CIMs finden Sie unter ***Unterstützte CIMs und Betriebssysteme (Zielserver)*** (auf Seite 309).
2. Schließen Sie den HD15-Videostecker des CIM an den Videoport des Zielservers an. Stellen Sie sicher, dass die Grafikeinstellungen Ihres Zielservers bereits so konfiguriert sind, dass eine unterstützte Auflösung und Aktualisierungsfrequenz eingestellt sind. Stellen Sie bei Servern von Sun weiterhin sicher, dass die Grafikkarte Ihres Zielservers so eingestellt ist, dass Standard-VGA (H- und V-Synchronisierung) und nicht Composite-Synchronisierung ausgegeben wird.
3. Schließen Sie den Tastatur-/Mausstecker des CIM an die entsprechenden Ports des Zielservers an. Verwenden Sie ein standardmäßiges Straight-Through-UTP-Kabel (Kat. 5/5e/6), um das CIM mit einem verfügbaren Serverport auf der Rückseite Ihres Dominion KX II-Geräts zu verbinden.

Hinweis: D2CIM-USB G2 verfügt über einen kleinen Schiebeschalter auf der Rückseite des CIM. Schalten Sie den Schalter in Position "B" für PC-basierte USB-Zielserver. Schalten Sie den Schalter in Position "S" für Sun-USB-Zielserver.

Eine neue Switch-Position wird erst wirksam, wenn das CIM aus- und wieder eingeschaltet wird. Um das CIM aus- und wieder einzuschalten, entfernen Sie den USB-Stecker vom Zielserver und schließen Sie ihn nach einigen Sekunden erneut an.

Schritt 4: Konfigurieren von Dominion KX II

Wenn Sie das Dominion KX II-Gerät zum ersten Mal starten, müssen Sie einige Konfigurationseinstellungen über die lokale Dominion KX II-Konsole vornehmen:

- Ändern des Standardkennworts
- Zuweisen der IP-Adresse
- Benennen der KVM-Zielserver

Ändern des Standardkennworts

Dominion KX II wird mit einem Standardkennwort geliefert. Beim ersten Starten des Dominion KX II müssen Sie dieses Kennwort ändern.

So ändern Sie das Standardkennwort:

1. Schalten Sie das Dominion KX II-Gerät mithilfe des Netzschalters auf der Rückseite des Geräts ein. Warten Sie, bis die Dominion KX II-Einheit hochgefahren ist. (Bei Abschluss des Bootvorgangs wird ein Tonsignal ausgegeben.)
2. Nach dem Bootvorgang des Dominion KX II wird die lokale Konsole auf dem Monitor angezeigt, der an den lokalen Port des Dominion KX II angeschlossen ist. Geben Sie den standardmäßigen Benutzernamen (admin) und das standardmäßige Kennwort (raritan) ein, und klicken Sie anschließend auf "Login" (Anmelden). Das Fenster "Change Password" (Kennwort ändern) wird angezeigt.
3. Geben Sie in das Feld "Old Password" (Altes Kennwort) Ihr altes Kennwort (raritan) ein.
4. Geben Sie im Feld "New Password" (Neues Kennwort) das neue Kennwort ein, und anschließend im Feld "Confirm New Password" (Neues Kennwort bestätigen) erneut. Ein Kennwort kann aus bis zu 64 alphanumerischen Zeichen der englischen Sprache und aus Sonderzeichen bestehen.
5. Klicken Sie auf "Apply" (Übernehmen).
6. Die erfolgreiche Änderung des Kennworts wird bestätigt. Klicken Sie auf OK. Die Seite "Port Access" (Portzugriff) wird angezeigt.

Hinweis: Das Standardkennwort kann auch mittels des Multi-Platform-Clients (MPC) von Raritan geändert werden.



Zuweisen einer IP-Adresse

Im Folgenden wird das Zuweisen einer IP-Adresse auf der Seite "Network Settings" (Netzwerkeinstellungen) beschrieben. Umfassende Informationen zu allen Feldern sowie zur Funktionsweise dieser Seite finden Sie unter ***Netzwerkeinstellungen*** (auf Seite 157).

1. Wählen Sie "Device Settings" > "Network" (Geräteeinstellungen > Netzwerk) aus. Die Seite "Network Settings" (Netzwerkeinstellungen) wird angezeigt.
2. Geben Sie einen aussagekräftigen Namen für Ihr Dominion KX II-Gerät an. Verwenden Sie dazu bis zu 32 gültige Sonderzeichen und keine Leerzeichen.
3. Geben Sie im Bereich "IPv4" die entsprechenden IPv4-spezifischen Netzwerkeinstellungen ein oder wählen Sie diese aus:
   a. Geben Sie eine IP-Adresse ein, falls erforderlich. Die Standard-IP-Adresse lautet 192.168.0.192.
   b. Geben Sie die Subnetzmaske ein. Die Standardsubnetzmaske lautet 255.255.255.0.
   c. Geben Sie das Standardgateway ein, wenn in der Dropdownliste unter "IP Auto Configuration" (Automatische IP-Konfiguration) "None" (Keine) ausgewählt ist.
   d. Geben Sie den Namen des bevorzugten DHCP-Hosts ein, wenn in der Dropdownliste unter "IP Auto Configuration" (Automatische IP-Konfiguration) "DHCP" ausgewählt ist.
   e. Wählen Sie "IP Auto Configuration" (Automatische IP-Konfiguration) aus. Folgende Optionen stehen zur Verfügung:
   - None (Static IP) [Keine (Statisches IP)] – Bei Auswahl dieser Option müssen Sie die Netzwerkparameter manuell angeben.

     Diese Option wird empfohlen, da Dominion KX II ein Infrastrukturgerät ist, dessen IP-Adresse sich nicht ändern sollte.
   - DHCP – Dynamic Host Configuration Protocol wird von Netzwerkcomputern (Clients) verwendet, um eindeutige IP-Adressen und andere Parameter von einem DHCP-Server zu erhalten.

     Bei Auswahl dieser Option gibt der DHCP-Server die Netzwerkparameter an. Bei Verwendung von DHCP geben Sie den Namen des bevorzugten Hosts ein (nur DHCP) (maximal 63 Zeichen).
4. Wenn IPv6 verwendet werden soll, geben Sie im Bereich "IPv6" die entsprechenden IPv6-spezifischen Netzwerkeinstellungen ein oder wählen Sie diese aus:
   a. Aktivieren Sie das Kontrollkästchen "IPv6", um die Felder in diesem Bereich zu aktivieren.

b. Geben Sie eine globale/eindeutige IP-Adresse ein. Dies ist die IP-Adresse, die dem Dominion KX II zugeordnet ist.

c. Geben Sie die Präfixlänge ein. Dies ist die Anzahl der Bits, die in der IPv6-Adresse verwendet werden.

d. Geben Sie die IP-Adresse des Gateway ein.

e. Link-Local-IP-Adresse. Diese Adresse wird dem Gerät automatisch zugewiesen. Sie wird zum Erkennen von Nachbarn verwendet oder wenn keine Router verfügbar sind. **Read-Only (Lesezugriff)**

f. Zonen-ID. Hierdurch wird das Gerät identifiziert, dem die Adresse zugeordnet ist. **Read-Only (Lesezugriff)**

g. Wählen Sie "IP Auto Configuration" (Automatische IP-Konfiguration) aus. Folgende Optionen stehen zur Verfügung:

- None (Keine) – Wählen Sie diese Option aus, wenn Sie keine automatische IP-Konfiguration wünschen, sondern die IP-Adresse lieber selbst festlegen (statisches IP). Diese Option ist voreingestellt und wird empfohlen.

  Wenn für "IP auto configuration" (Automatische IP-Konfiguration) "None" (Keine) ausgewählt ist, sind die folgenden "Network Basic Settings" (Basisnetzwerkeinstellungen) aktiviert: "Global/Unique IP Address" (Globale/Eindeutige IP-Adresse), "Prefix Length" (Präfixlange) und "Gateway IP Address" (Gateway-IP-Adresse) ermöglichen Ihnen die manuelle IP-Konfiguration.

- Router Discovery (Router-Erkennung) – Verwenden Sie diese Option, um IPv6-Adressen, deren Signifikanz "Global" oder "Unique Local" (Lokal eindeutig) ist und über der von Link Local liegt, welche nur für ein direkt verbundenes Subnetz gültig ist, automatisch zuzuordnen.

5. Wenn DHCP ausgewählt ist, wählen Sie "Obtain DNS Server Address Automatically" (DNS-Serveradresse automatisch abrufen) aus, um diese Funktion zu aktivieren. Wenn die DNS-Serveradresse automatisch abgerufen wird, werden die vom DHCP-Server bereitgestellten DNS-Informationen verwendet.

6. Wenn "Use the Following DNS Server Addresses" (Die folgenden DNS-Serveradressen verwenden) ausgewählt ist, werden die in diesem Abschnitt eingegebenen Adressen für die Verbindung zum DNS-Server verwendet, unabhängig davon, ob DHCP ausgewählt wurde.

   Geben Sie die folgenden Informationen ein, wenn die Option "Following DNS Server Addresses" (Folgende DNS-Serveradressen) ausgewählt wurde. Diese Adressen sind die primären und sekundären DNS-Adressen, die verwendet werden, wenn die primäre DNS-Serververbindung aufgrund eines Ausfalls getrennt wird.



   a. Primary DNS Server IP Address (IP-Adresse des primären DNS-Servers)
   b. Secondary DNS-Server IP Address (IP-Adresse des sekundären DNS-Servers)
7. Klicken Sie abschließend auf OK. Das Dominion KX II-Gerät ist jetzt über das Netzwerk zugänglich.

Weitere Informationen zur Konfiguration dieses Bereichs der Seite "Network Settings" (Netzwerkeinstellungen) finden Sie unter ***LAN-Schnittstelleneinstellungen*** (auf Seite 162).

Hinweis: Bei manchen Umgebungen gibt die Standardeinstellung "Autodetect" (automatische Aushandlung) für "LAN Interface Speed & Duplex" (LAN-Schnittstellengeschwindigkeit und Duplex) die Netzwerkparameter nicht richtig vor, was zu Netzwerkproblemen führen kann. Wählen Sie in einem solchen Fall im Feld "LAN Interface Speed & Duplex" des Dominion KX II den Wert "100 Mbps/Full Duplex" (100 Mbit/s/Vollduplex) (bzw. die geeignete Option für Ihr Netzwerk) aus, um dieses Problem zu beheben. Weitere Informationen finden Sie auf der Seite **Network Settings** *(siehe "***Netzwerkeinstellungen***" auf Seite 157) (Netzwerkeinstellungen).*

Benennen der Zielserver

▶ So benennen Sie die Zielserver:

1. Schließen Sie alle Zielserver an, falls dies noch nicht geschehen ist. Weitere Einzelheiten finden Sie unter ***Schritt 3: Anschließen der Geräte*** (siehe "***Schritt 3: Anschließen der Geräte***" auf Seite 30) für eine Beschreibung zum Anschließen der Geräte.
2. Wählen Sie in der lokalen Konsole des Dominion KX II "Device Settings" > "Port Configuration" (Geräteeinstellungen > Portkonfiguration) aus. Die Seite "Port Configuration" (Portkonfiguration) wird angezeigt.
3. Klicken Sie auf den Portnamen des Zielservers, den Sie umbenennen möchten. Die Seite "Port" wird angezeigt.
4. Weisen Sie dem mit diesem Port verbundenen Server einen Namen zu. Der Name darf maximal 32 alphanumerische Zeichen oder Sonderzeichen umfassen.
5. Klicken Sie auf OK.

Gültige Sonderzeichen für Zielnamen

Zeichen	Beschreibung	Zeichen	Beschreibung
!	Ausrufezeichen	;	Strichpunkt
"	Doppeltes Anführungszeiche	=	Gleichheitszeiche



Zeichen	Beschreibung	Zeichen	Beschreibung
	n		n
#	Raute	>	Größer-als-Zeiche n
$	Dollarzeichen	?	Fragezeichen
%	Prozentzeichen	@	At-Zeichen
&	Kaufmännisches Und	[	Linke eckige Klammer
(	Linke runde Klammer	\	Umgekehrter Schrägstrich
)	Rechte runde Klammer	]	Rechte eckige Klammer
*	Sternchen	^	Zirkumflexzeichen
+	Pluszeichen	_	Unterstreichungsz eichen
,	Komma	`	Graviszeichen
-	Bindestrich	{	Linke geschweifte Klammer
.	Punkt	|	Senkrechter Strich
/	Schrägstrich	}	Rechte geschweifte Klammer
<	Kleiner-als-Zeiche n	~	Tilde
:	Doppelpunkt		



Festlegen der automatischen Netzteilerkennung

Dominion KX II bietet zwei Netzteile und kann den Status dieser Netzteile automatisch erkennen und entsprechende Benachrichtigungen ausgeben. Mit der korrekten Konfiguration stellen Sie sicher, dass Dominion KX II die entsprechenden Benachrichtigungen bei einem Ausfall der Stromversorgung sendet.

Die Seite "Power Supply Setup" (Netzteilkonfiguration) ist so konfiguriert, dass automatisch beide Netzteile erkannt werden, wenn diese verwendet werden. Wenn in Ihrer Konfiguration nur ein Netzteil verwendet wird, können Sie die automatische Erkennung auf der Seite "Power Supply Setup" (Netzteilkonfiguration) deaktivieren.

▶ So aktivieren Sie die automatische Erkennung für die verwendeten Netzteile:

1. Wählen Sie "Device Settings > Power Supply Setup" (Geräteeinstellungen und Netzteilkonfiguration) aus. Die Seite "Power Supply Setup" (Netzteilkonfiguration) wird angezeigt.
2. Wenn die Stromversorgung über das Netzteil 1 erfolgt (ganz links auf der Rückseite des Geräts), wählen Sie die Option "PowerIn1 Auto Detect" (Netzteil 1 – Automatische Erkennung) aus.
3. Wenn die Stromversorgung über das Netzteil 2 erfolgt (ganz rechts auf der Rückseite des Geräts), wählen Sie die Option "PowerIn2 Auto Detect" (Netzteil 2 – Automatische Erkennung) aus.
4. Klicken Sie auf OK.

Hinweis: Wenn eines dieser Kontrollkästchen aktiviert ist und das entsprechende Netzteil zurzeit nicht angeschlossen ist, leuchtet die Stromversorgungs-LED-Anzeige auf der Vorderseite des Geräts rot.

▶ So deaktivieren Sie die automatische Erkennung für das nicht verwendete Netzteil:

1. Wählen Sie in der lokalen Konsole des Dominion KX II "Device Settings" > "Power Supply Setup" (Geräteeinstellungen > Netzteilkonfiguration) aus. Die Seite "Power Supply Setup" (Netzteilkonfiguration) wird angezeigt.
2. Deaktivieren Sie die automatische Erkennung für das nicht verwendete Netzteil.

Weitere Informationen finden Sie unter ***Netzteilkonfiguration*** (auf Seite 185).

Hinweis für CC-SG-Benutzer

Wenn Sie Dominion KX II in einer CC-SG-Konfiguration verwenden, führen Sie die Installationsschritte aus und befolgen anschließend die Anweisungen im **CommandCenter Secure Gateway-Benutzerhandbuch**, **Administratorhandbuch** oder **Implementierungshandbuch** (Zu finden auf der Website von Raritan (www.raritan.com) unter "Support").

Hinweis: Das restliche Hilfedokument gilt in erster Linie für die Bereitstellung von Dominion KX II-Geräten ohne die Integrationsfunktion von CC-SG.

Remoteauthentifizierung

Hinweis für CC-SG-Benutzer

Wenn Dominion KX II von CommandCenter Secure Gateway gesteuert wird, authentifiziert CC-SG Benutzer und Gruppen, mit Ausnahme von lokalen Benutzern, für die der Zugriff auf den lokalen Port erforderlich ist. Steuert CC-SG die Dominion KX II-Einheit, erfolgt die Authentifizierung von Benutzern des lokalen Ports über die lokale Benutzerdatenbank oder den für Dominion KX II konfigurierten Remote-Authentifizierungsserver (LDAP/LDAPS oder RADIUS). Sie werden nicht über die CC-SG-Benutzerdatenbank authentifiziert.

Weitere Informationen zur CC-SG-Authentifizierung finden Sie im CommandCenter Secure Gateway-Benutzerhandbuch, im Administratorhandbuch oder im Bereitstellungshandbuch, die im Bereich "Support" auf der ***Raritan-Website http://www.raritan.com*** heruntergeladen werden können.

Unterstützte Protokolle

Zur Vereinfachung der Verwaltung von Benutzernamen und Kennwörtern bietet Dominion KX II die Möglichkeit, Authentifizierungsanforderungen an einen externen Authentifizierungsserver weiterzuleiten. Zwei externe Authentifizierungsprotokolle werden unterstützt: LDAP/LDAPS und RADIUS.

Hinweis zu Microsoft Active Directory

Microsoft® Active Directory® verwendet nativ das LDAP/LDAPS-Protokoll und kann als LDAP/LDAPS-Server und Authentifizierungsquelle für Dominion KX II fungieren. Bei Verwendung der IAS-Komponente (Internetautorisierungsserver) kann ein Microsoft Active Directory-Server auch als RADIUS-Authentifizierungsquelle dienen.



Erstellen von Benutzergruppen und Benutzern

Im Rahmen der Erstkonfiguration müssen Sie Benutzergruppen und Benutzer definieren, damit Benutzer auf Dominion KX II zugreifen können.

Dominion KX II verwendet im System bereits vorhandene Standardbenutzergruppen und ermöglicht es Ihnen, Gruppen zu erstellen und entsprechende Berechtigungen für sie festzulegen.

Für den Zugriff auf Dominion KX II sind ein Benutzername und ein Kennwort erforderlich. Anhand dieser Informationen werden Benutzer authentifiziert, die versuchen, auf Dominion KX II zuzugreifen.

Weitere Informationen zum Hinzufügen oder Bearbeiten von Benutzergruppen und Benutzern finden Sie unter Benutzerverwaltung.

Schritt 5 (Optional): Konfigurieren der Tastatursprache

Hinweis: Dieser Schritt ist nicht erforderlich, wenn Sie eine US-/internationale Tastatur verwenden.

Wenn Sie eine andere Tastatur verwenden, muss diese für die jeweilige Sprache konfiguriert werden. Außerdem muss die Tastatursprache für das Client-Gerät mit der der KVM-Zielserver übereinstimmen.

Weitere Informationen zum Ändern des Tastaturlayouts finden Sie in der Dokumentation Ihres Betriebssystems.

Ändern des Tastatur-Layout-Codes (Sun-Zielgeräte)

Gehen Sie folgendermaßen vor, wenn Sie ein DCIM-SUSB verwenden und das Tastaturlayout auf eine andere Sprache ändern möchten.

So ändern Sie den Tastaturlayoutcode (nur DCIM-SUSB):

1. Öffnen Sie auf der Sun™-Workstation ein Texteditorfenster.
2. Vergewissern Sie sich, dass die Taste "Num Lock" aktiviert ist, und drücken Sie die linke Strg-Taste und die Taste "Entf" auf der Tastatur. Die LED der Feststelltaste beginnt zu blinken, was darauf hindeutet, dass sich das CIM im Modus zum Ändern des Layoutcodes befindet. Im Textfenster wird Folgendes angezeigt: `Raritan Computer, Inc. Current keyboard layout code = 22h (US5 UNIX)` [Raritan Computer, Inc. Aktueller Tastaturlayoutcode = 22h (US5 UNIX)].
3. Geben Sie den gewünschten Layoutcode ein (für eine japanische Tastatur beispielsweise *31*).
4. Drücken Sie die Eingabetaste.
5. Schalten Sie das Gerät aus und wieder ein. Das DCIM-SUSB wird zurückgesetzt (Aus- und Einschalten).

6. Überprüfen Sie, ob die Zeichen korrekt sind.



Kapitel 3 Arbeiten mit Zielservern

In diesem Kapitel

Oberflächen

Dominion KX II bietet Ihnen verschiedene Benutzeroberflächen, über die Sie jederzeit und überall einfach auf die Einheit zugreifen können. Dazu zählen die lokale Dominion KX II-Konsole, die Dominion KX II-Remotekonsole und der Multi-Platform-Client (MPC). In der folgenden Tabelle werden diese Oberflächen und ihre Nutzung für den Zielserverzugriff und die lokale sowie die Remoteverwaltung erläutert:

Benutzeroberfläche	**Lokal**		**Remote**	
	Access (Zugriff)	**Admin**	**Access (Zugriff)**	**Admin**
Lokale Dominion KX II-Konsole	✓	✓		
Dominion KX II-Remotekonsole			✓	✓
Virtual KVM Client			✓	
Multi-Platform-Client (MPC)			✓	✓
Active KVM Client (AKC)			✓	✓

Die folgenden Abschnitte des Hilfedokuments enthalten Informationen zur Verwendung spezieller Oberflächen, um auf Dominion KX II zuzugreifen und Zielgeräte zu verwalten.

- Lokale Konsole
- Remotekonsole
- Virtual KVM Client
- Multi-Platform-Client

Oberfläche der lokalen Dominion KX II-Konsole

Am Serverschrank erfüllt Dominion KX II über die lokale Dominion KX II-Konsole standardmäßige KVM-Management- und Verwaltungsfunktionen. Die lokale Dominion KX II-Konsole stellt eine direkte KVM-Verbindung (analog) mit den angeschlossenen Servern her. Die Leistung ist mit der Leistung bei einer direkten Verbindung mit der Tastatur, der Maus und den Videoports des Servers identisch.

Die grafischen Benutzeroberflächen der lokalen Dominion KX II-Konsole und der Dominion KX II-Remotekonsole verfügen über zahlreiche Gemeinsamkeiten. Auf die Unterschiede wird in diesem Hilfedokument hingewiesen.

Die Dominion KX II-Option "Local Console Factory Reset" (Werksrücksetzung der lokalen Konsole) ist bei der lokalen Dominion KX II-Konsole verfügbar, jedoch nicht bei der Dominion KX II-Remotekonsole.

Oberfläche der Dominion KX II-Remotekonsole

Die Dominion KX II-Remotekonsole ist eine browserbasierte grafische Benutzeroberfläche, mit der Sie sich an KVM-Zielservern und seriellen Zielgeräten, die mit Dominion KX II verbunden sind, anmelden und Dominion KX II von einem Remotestandort aus verwalten können.

Die Dominion KX II-Remotekonsole bietet eine digitale Verbindung mit den angeschlossenen KVM-Zielservern. Wenn Sie sich über die Dominion KX II-Remotekonsole bei einem KVM-Zielserver anmelden, wird ein Fenster für den Virtual KVM Client geöffnet.

Die grafischen Benutzeroberflächen der lokalen Dominion KX II-Konsole und der Dominion KX II-Remotekonsole verfügen über zahlreiche Gemeinsamkeiten. Auf die Unterschiede wird in diesem Benutzerhandbuch hingewiesen. Die folgenden Optionen stehen nur für die Dominion KX II-Remotekonsole, nicht jedoch für die lokale Dominion KX II-Konsole zur Verfügung:

- Virtual Media (Virtuelle Medien)
- Favorites (Favoriten)
- Backup/Restore (Sicherung/Wiederherstellung)
- Firmware Upgrade (Firmwareaktualisierung)
- Upgrade Report (Aktualisierungsbericht)
- Diagnostics (Diagnose)
- USB-Profilauswahl
- USB Profile Management (USB-Profilverwaltung)
- SSL-Zertifikate



Starten der Dominion KX II-Remotekonsole

Wichtig: Unabhängig vom verwendeten Browser müssen Popups für die IP-Adresse des Dominion-Geräts zugelassen werden, damit die Dominion KX II-Remotekonsole gestartet werden kann.

Abhängig von den Browser- und Sicherheitseinstellungen werden möglicherweise verschiedene Sicherheits- und Zertifikatwarnungen angezeigt. Sie müssen diese Warnungen bestätigen, um die Dominion KX II-Remotekonsole zu starten.

Sie können die Zahl der Warnmeldungen zur Sicherheit und zu Zertifikaten für zukünftige Anmeldungen reduzieren, indem Sie darin die folgenden Kontrollkästchen aktivieren:

- In the future, do not show this warning (Diese Warnung nicht mehr anzeigen).
- Always trust content from this publisher (Inhalt von diesem Herausgeber immer vertrauen).

So starten Sie die Dominion KX II-Remotekonsole:

1. Melden Sie sich bei einer Workstation an, die eine Netzwerkverbindung zu Dominion KX II herstellen kann und auf der Java Runtime Environment installiert ist (JRE ist auf der ***Java-Website http://java.sun.com/*** verfügbar).
2. Starten Sie einen unterstützten Webbrowser, z. B. Internet Explorer (IE) oder Firefox.
3. Geben Sie den folgenden URL ein: *http://IP-ADRESSE*, wobei IP-ADRESSE die dem Dominion KX II zugewiesene IP-Adresse ist. Sie können auch "https" verwenden, den vom Administrator zugewiesenen DNS-Namen des Dominion KX II (sofern ein DNS-Server konfiguriert wurde), oder einfach die IP-Adresse im Browser eingeben (Dominion KX II leitet die IP-Adresse stets von HTTP zu HTTPS um). Die Anmeldeseite wird angezeigt.
4. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein. Wenn Sie sich zum ersten Mal anmelden, geben Sie den/das werkseitig voreingestellte(n) Benutzernamen (admin) und Kennwort (raritan, beides kleingeschrieben) ein. Sie werden aufgefordert, das Standardkennwort zu ändern. Weitere Informationen finden Sie unter ***Ändern des Standardkennworts*** (auf Seite 34). Klicken Sie auf "Login" (Anmelden).

   Hinweis: Wenn es für Ihren Administrator erforderlich ist, dass Sie eine Sicherheitsvereinbarung lesen und/oder akzeptieren, um auf das Gerät zuzugreifen, wird eine Sicherheitsmeldung angezeigt, nachdem Sie Ihre Anmeldedaten eingegeben und auf "Login" (Anmelden) geklickt haben.



Weitere Informationen zu den Dominion KX II-Funktionen, die über die Remotekonsole verfügbar sind, finden Sie unter ***Virtual KVM Client*** (auf Seite 63).

Oberfläche und Navigation

Layout der Dominion KX II-Konsole

Die Dominion KX II-Remotekonsole und die lokale Dominion KX II-Konsole bieten für die Konfiguration und Verwaltung eine HTML-Oberfläche (webbasiert) sowie eine Liste und Auswahl der Zielserver. Die Optionen befinden sich auf verschiedenen Registerkarten.

Nachdem Sie sich erfolgreich angemeldet haben, wird die Seite "Port Access" (Portzugriff) angezeigt, in der alle Ports mit ihrem Status und ihrer Verfügbarkeit aufgeführt sind. Auf der Seite werden zwei Registerkarten angezeigt (für die Ansicht nach Port oder die Ansicht nach Gruppe). Klicken Sie auf eine Spaltenüberschrift, um die Ports nach Port Number (Portnummer), Port Name (Portname), Status (Up/Down) [Status (Ein oder Aus)] und Availability (Idle, Connected, Busy, Unavailable, Connecting) [Verfügbarkeit (Inaktiv, Verbunden, Verwendet, Nicht verfügbar und Verbindung wird hergestellt)] zu sortieren. Weitere Informationen finden Sie unter ***Seite "Port Access" (Portzugriff)*** (auf Seite 50).



Linker Bildschirmbereich

Der linke Bildschirmbereich der Dominion KX II-Oberfläche enthält folgende Informationen. Beachten Sie, dass die Anzeige einiger Informationen abhängig vom Benutzer, von der verwendeten Funktion usw. ist. Diese bedingten Informationen werden nachfolgend aufgeführt.

Informationen	Beschreibung	Anzeige
Zeit & Sitzung	Datum und Uhrzeit, wann die aktuelle Sitzung begonnen hat.	Immer
Benutzer	Benutzername	Immer
Status	Der aktuelle Status der Anwendung, entweder inaktiv oder aktiv. Bei Inaktivität zeichnet die Anwendung die Uhrzeit der inaktiven Sitzung auf und zeigt diese an.	Immer
Ihre IP	Die für den Zugriff auf Dominion KX II verwendete IP-Adresse.	Immer
Letzte Anmeldung	Datum und Uhrzeit der letzten Anmeldung.	Immer
Unter CC-SG-Verwaltung	Die IP-Adresse des CC-SG-Gertäts, das Dominion KX II verwaltet.	Wenn Dominion KX II von CC-SG verwaltet wird.
Device Information (Geräteinformationen)	Informationen zum verwendeten Dominion KX II.	Immer
Gerätename	Dem Gerät zugewiesener Name.	Immer
IP-Adresse	Die IP-Adresse des Dominion KX II.	Immer
Firmware	Aktuelle Version der Firmware.	Immer
Gerätemodell	Modell des Dominion KX II	Immer
Netzwerk	Der dem aktuellen Netzwerk zugewiesene Name.	Immer

Informationen	Beschreibung	Anzeige
Stromeingang1	Status der Stromversorgung 1. Entweder ein- oder ausgeschaltet.	Wenn angeschlossen.
Stromeingang2	Status der Stromversorgung 2. Entweder ein- oder ausgeschaltet.	Wenn angeschlossen.
Als Basis oder als Schicht konfiguriert	Wenn Sie eine Schichtkonfiguration verwenden, wird hier angezeigt, ob es sich bei Dominion KX II, auf das Sie zugreifen, um das Basis- oder Schichtgerät handelt.	Wenn Dominion KX II Teil einer Schichtkonfiguration ist.
Portstatus	Die Status der Ports, die von Dominion KX II verwendet werden.	Immer
Verbundene Benutzer	Die Benutzer, identifiziert durch Benutzername und IP-Adresse, die aktuell mit Dominion KX II verbunden sind.	Immer
Hilfe – Benutzerhandbuch	Verknüpfung zur Online-Hilfe.	Immer
Bevorzugte Geräte	Siehe ***Verwalten von Favoriten*** (auf Seite 54).	Immer
FIPS-Modus	FIPS-Modus: Aktiviertes SSL-Zertifikat: Kompatibel mit FIPS-Modus	Wenn FIPS aktiviert ist.



Navigation in der Dominion KX II-Konsole

In den Oberflächen der Dominion KX II-Konsolen haben Sie viele Möglichkeiten für die Navigation und Auswahl.

▶ Für die Auswahl von Optionen stehen folgende Möglichkeiten zur Verfügung:

- Klicken Sie auf eine Registerkarte. Eine Seite mit verfügbaren Optionen wird angezeigt.
- Zeigen Sie mit dem Cursor auf eine Registerkarte und wählen Sie die gewünschte Option aus dem Menü aus.
- Klicken Sie in der angezeigten Menühierarchie (den sogenannten "Breadcrumbs") direkt auf die gewünschte Option.

▶ So blättern Sie durch Seiten, die größer als der Bildschirm sind:

- Verwenden Sie die Bild-Auf- und Bild-Ab-Tasten der Tastatur.
- Verwenden Sie die Bildlaufleiste auf der rechten Seite.

Seite "Port Access" (Portzugriff)

Nachdem Sie sich erfolgreich bei der Dominion KX II-Remotekonsole angemeldet haben, wird die Seite "Port Access" (Portzugriff) angezeigt. Diese Seite enthält alle Dominion KX II-Ports, die angeschlossenen KVM-Zielserver sowie deren Status und Verfügbarkeit. Über die Seite "Port Access" (Portzugriff) haben Sie Zugriff auf die mit Dominion KX II verbundenen KVM-Zielserver. KVM-Zielserver sind Server, die Sie über das Dominion KX II-Gerät steuern möchten. Sie sind mit den Dominion KX II-Ports auf der Rückseite des Geräts verbunden.

Hinweis: Für jede Verbindung mit einem KVM-Zielserver wird eine neue Seite für den Virtual KVM Client geöffnet.

Wenn Sie eine Schichtkonfiguration verwenden, in der ein Dominion KX II-Basisgerät für den Zugriff auf mehrere andere Schichtgeräte verwendet wird, werden die Schichtgeräte auf der Seite "Port Access" (Portzugriff) angezeigt, wenn Sie auf das Symbol "Expand Arrow" (Pfeil erweitern) ► links neben dem Basisgerätenamen klicken. Weitere Informationen zu Schichten finden Sie unter ***Konfigurieren und Aktivieren von Schichten*** (auf Seite 167).

Auf der Seite "Port Access" (Portzugriff) werden außerdem Blade-Chassis angezeigt, die im Dominion KX II konfiguriert wurden. Das Blade-Chassis wird in einer erweiterbaren, hierarchischen Liste auf der Seite "Port Access" (Portzugriff) angezeigt, wobei das Blade-Chassis auf Stammebene der Hierarchie angezeigt und die einzelnen Blades unterhalb der Stammebene bezeichnet und angezeigt werden. Verwenden Sie das Symbol "Expand Arrow" (Pfeil erweitern) neben dem Stamm-Chassis, um die einzelnen Blades anzuzeigen.

Hinweis: Um das Blade-Chassis in hierarchischer Reihenfolge anzuzeigen, müssen für das Bladeserver-Chassis Blade-Chassis-Subtypen konfiguriert werden.

Standardmäßig wird die Registerkarte "View by Port" (Ansicht nach Port) auf der Seite "Port Access" (Portzugriff) angezeigt. Auf der Registerkarte "View by Group" (Ansicht nach Gruppe) werden Portgruppen angezeigt. Die Registerkarte kann erweitert werden, um die der Portgruppe zugewiesenen Ports anzuzeigen. Mithilfe der Registerkarte "View by Search" (Ansicht nach Suche) können Sie nach Portnamen suchen. Die Suchfunktion unterstützt die Verwendung eines Sternchens (*) als Platzhalter sowie die Verwendung vollständiger Namen und Teile von Namen.

► So verwenden Sie die Seite "Port Access" (Portzugriff):

1. Klicken Sie in der Dominion KX II-Remotekonsole auf die Registerkarte "Port Access" (Portzugriff). Die Seite "Port Access" (Portzugriff) wird angezeigt.



Die KVM-Zielserver werden zuerst nach Portnummer sortiert. Sie können die Anzeige so ändern, dass nach einer beliebigen Spalte sortiert wird.

- Port Number (Portnummer) – Die für das Dominion KX II-Gerät verfügbaren Ports werden beginnend mit 1 durchnummeriert. Beachten Sie, dass mit Powerstrips verbundene Ports hier nicht aufgeführt werden, was zu Lücken in der Portnummernabfolge führt.
- Port Name (Portname) – Der Name des Dominion KX II-Ports. Standardmäßig lautet dieser "Dominion-KX2-Port#", Sie können den Namen jedoch durch einen aussagekräftigeren ersetzen. Wenn Sie auf einen Portnamenlink klicken, wird das Menü "Port Action" (Portaktion) geöffnet.

Hinweis: Verwenden Sie für den Port (CIM)-Namen keine Auslassungszeichen (Apostroph).

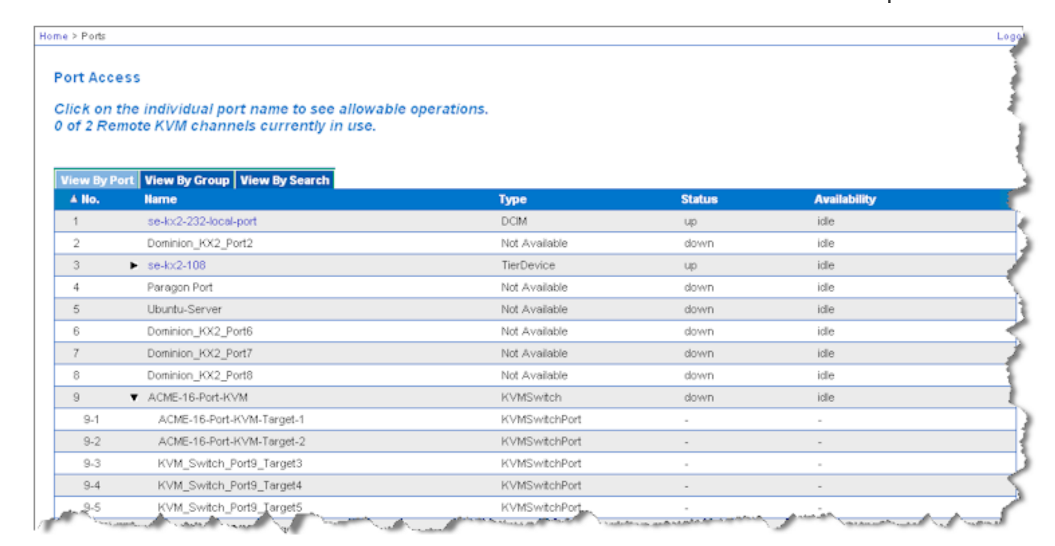
- Status – Der Status für Standardserver lautet entweder "Up" (Ein) oder "Down" (Aus).
- Type (Typ) – Der Server- oder CIM-Typ. Bei Blade-Chassis kann der Typ "Blade Chassis", "Blade", "BladeChassisAdmin" oder "BladeChassisURL" lauten. Der Typ kann auch "TierDevice" und "KVMSwitch" enthalten.
- Availability (Verfügbarkeit) – Für die Verfügbarkeit stehen die Werte Idle (Inaktiv), Connected (Verbunden), Busy (Verwendet) und Unavailable (Nicht verfügbar) zur Verfügung. Die Verfügbarkeit der Bladeserver lautet entweder "Shared" (Freigegeben) oder "Exclusive" (Exklusiv), wenn eine Verbindung zu diesem Blade besteht.

2. Klicken Sie auf "View by Port" (Ansicht nach Port), "View by Group" (Ansicht nach Gruppe) oder "View by Search" (Ansicht nach Suche), um zwischen den Ansichten zu wechseln.
3. Klicken Sie auf den Portnamen des Zielservers, auf den Sie zugreifen möchten. Das Menü "Port Action" (Portaktion) wird angezeigt. Informationen zu verfügbaren Menüoptionen finden Sie unter **Menü "Port Action" (Portaktion)** (auf Seite 52).
4. Wählen Sie im Menü "Port Action" (Portaktion) den gewünschten Menübefehl aus.



So ändern Sie die Sortierreihenfolge der Anzeige:

- Klicken Sie auf die Spaltenüberschrift, nach der sortiert werden soll. Die Liste der KVM-Zielserver wird nach dieser Spalte sortiert.



Menü "Port Action" (Portaktion)

Wenn Sie in der Liste "Port Access" (Portzugriff) auf einen Portnamen klicken, wird das Menü "Port Action" (Portaktion) angezeigt. Wählen Sie die gewünschte Menüoption für den Port aus. Beachten Sie, dass nur je nach Status und Verfügbarkeit des Ports aktuell verfügbare Optionen im Menü "Port Action" (Portaktion) aufgelistet werden.

- Connect (Verbinden) – Erstellt eine neue Verbindung mit dem Zielserver. Für die Dominion KX II-Remotekonsole wird eine neue ***Virtual KVM Client*** (auf Seite 63)-Seite angezeigt. Für die lokale Dominion KX II-Konsole wechselt die Anzeige von der lokalen Benutzeroberfläche hin zum Zielserver. Auf dem lokalen Port muss die Oberfläche der lokalen Dominion KX II-Konsole angezeigt werden, um den Wechsel durchführen zu können. Das Wechseln über Zugriffstasten ist vom lokalen Port auch verfügbar.

  Hinweis: Diese Option steht in der Dominion KX II-Remotekonsole für einen verfügbaren Port nicht zur Verfügung, wenn alle Verbindungen verwendet werden.

- Switch From (Wechseln von) – Wechselt von einer bestehenden Verbindung zum gewählten Port (KVM-Zielserver). Diese Menüoption ist nur für KVM-Zielgeräte verfügbar. Diese Option wird nur angezeigt, wenn der Virtual KVM Client geöffnet ist.

  Hinweis: Diese Menüoption steht auf der lokalen Dominion KX II-Konsole nicht zur Verfügung.



- Disconnect (Trennen) – Trennt diese Portverbindung und schließt die Seite des Virtual KVM Client für diesen Zielserver. Diese Menüoption ist nur für den Portstatus Up (Ein) und die Verfügbarkeit Connected (Verbunden) bzw. Up (Ein) und Busy (Verwendet) verfügbar.

Hinweis: Diese Menüoption steht auf der lokalen Dominion KX II-Konsole nicht zur Verfügung. Sie können die Verbindung zum gewechselten Zielgerät auf der lokalen Konsole nur trennen, indem Sie die Zugriffstaste verwenden.

- Power On (Strom ein) – Versorgt den Zielserver über die zugeordnete Steckdose mit Strom. Diese Option wird nur angezeigt, wenn mindestens eine Stromzuordnung für das Zielgerät besteht.
- Power Off (Strom aus) – Unterbricht die Stromversorgung des Zielservers über die zugeordneten Steckdosen. Diese Option wird nur angezeigt, wenn mindestens eine Stromzuordnung für das Zielgerät besteht, wenn dieses eingeschaltet ist [Portstatus Up (Ein)] und wenn der Benutzer über die Berechtigung verfügt, diesen Dienst zu nutzen.
- Power Cycle (Aus- und Einschalten) – Schaltet den Zielserver über die zugeordneten Steckdosen aus und wieder ein. Diese Option wird nur angezeigt, wenn mindestens eine Stromzuordnung für das Zielgerät besteht und wenn der Benutzer über die Berechtigung verfügt, diesen Dienst zu nutzen.

Verwalten von Favoriten

Mithilfe des Features "Favorites" (Favoriten) können Sie die häufig verwendeten Geräte organisieren und schnell darauf zugreifen. Der Bereich "Favorite Devices" (Bevorzugte Geräte) befindet sich links unten (Randleiste) auf der Seite "Port Access" (Portzugriff). Hier haben Sie folgende Möglichkeiten:

- Erstellen und Verwalten einer Liste bevorzugter Geräte
- Schnelles Zugreifen auf häufig verwendete Geräte
- Auflisten der Favoriten nach Gerätename, IP-Adresse oder DNS-Hostname
- Erkennen von Dominion KX II-Geräten im Subnetz (vor und nach der Anmeldung)
- Abrufen erkannter Dominion KX II-Geräte vom verbundenen KX-Gerät (nach der Anmeldung)

Hinweis: Diese Funktion steht nur auf der Dominion KX II-Remotekonsole (nicht auf der lokalen Dominion KX II-Konsole oder auf dem AKC) zur Verfügung.

So greifen Sie auf ein bevorzugtes Dominion KX II-Gerät zu:

- Klicken Sie auf den unterhalb von "Favorite Devices" (Bevorzugte Geräte) aufgeführten Namen des Geräts. Ein neues Browserfenster wird geöffnet.

So zeigen Sie die Favoriten nach Name an:

- Klicken Sie auf "Display by Name" (Nach Name anzeigen).

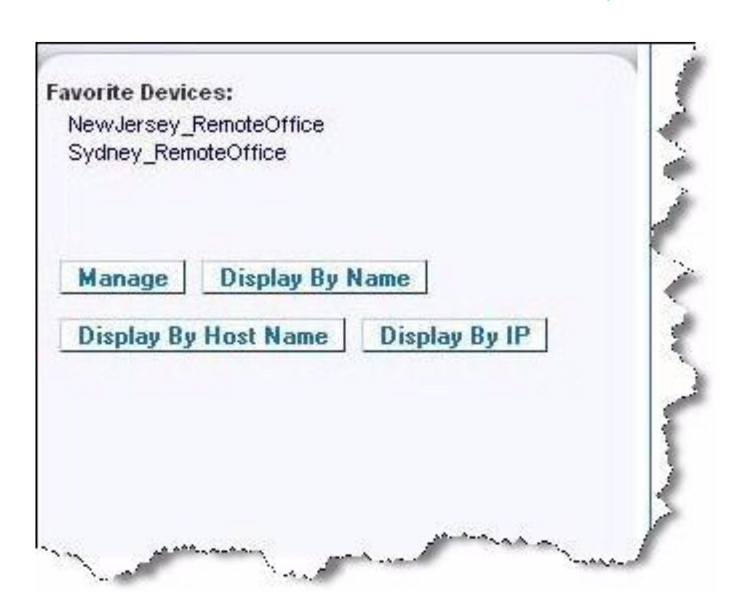
So zeigen Sie die Favoriten nach IP-Adresse an:

- Klicken Sie auf "Display by IP" (Nach IP anzeigen).

So zeigen Sie die Favoriten nach Hostname an:

- Klicken Sie auf "Display by Host Name" (Nach Hostname anzeigen).





Hinweis: Sowohl IPv4- als auch IPv6-Adressen werden unterstützt.

Seite "Manage Favorites" (Favoriten verwalten)

So öffnen Sie die Seite "Manage Favorites" (Favoriten verwalten):

- Klicken Sie auf die Schaltfläche "Manage" (Verwalten) im linken Bildschirmbereich. Die Seite "Manage Favorites" (Favoriten verwalten) wird angezeigt. Diese Seite enthält die folgenden Optionen:

Option	Verwendungszweck
Favorites List (Favoritenliste)	Verwalten einer Liste bevorzugter Geräte
Discover Devices - Local Subnet (Geräte erkennen – Lokales Subnetz)	Erkennen von Raritan-Geräten auf dem lokalen Subnetz des Client-PC.
Discover Devices - Dominion KX II Subnet (Geräte erkennen – Dominion KX II-Subnetz)	Erkennen der Raritan-Geräte im Subnetz des Dominion KX II-Geräts
Add New Device to Favorites (Neues Gerät zu Favoriten hinzufügen)	Hinzufügen, Bearbeiten und Löschen von Geräten in der Favoritenliste

Seite "Favorites List" (Favoritenliste)

Auf der Seite "Favorites List" (Favoritenliste) können Sie der Favoritenliste Geräte hinzufügen und in der Favoritenliste aufgeführte Geräte bearbeiten oder löschen.

So öffnen Sie die Seite "Favorites List" (Favoritenliste):

- Wählen Sie "Manage" > "Favorites List" (Verwalten > Favoritenliste) aus. Die Seite "Favorites List" (Favoritenliste) wird angezeigt.

Erkennen von Geräten auf dem lokalen Subnetz

Mit dieser Option werden die Geräte auf dem lokalen Subnetz erkannt. Dieses ist das Subnetz, auf dem die Dominion KX II-Remotekonsole ausgeführt wird. Auf die Geräte können Sie direkt von dieser Seite aus zugreifen, oder Sie können sie zur Favoritenliste hinzufügen. Siehe***Seite "Favorites List"*** (siehe "***Seite "Favorites List" (Favoritenliste)***" auf Seite 56) (Favoritenliste).

So finden Sie Geräte im lokalen Subnetz:

1. Wählen Sie "Manage" > "Discover Devices – Local Subnet" (Verwalten > Geräte erkennen – Lokales Subnetz) aus. Die Seite "Discover Devices – Local Subnet" (Geräte erkennen – Lokales Subnetz) wird angezeigt.
2. Wählen Sie den entsprechenden Erkennungsport aus:
   - Wenn Sie den Standarderkennungs-Port verwenden möchten, aktivieren Sie das Kontrollkästchen "Use Default Port 5000" (Standard-Port 5000 verwenden).
   - Wenn Sie einen anderen Erkennungsport verwenden möchten, gehen Sie wie folgt vor:

   a. Deaktivieren Sie das Kontrollkästchen "Use Default Port 5000" (Standard-Port 5000 verwenden).

   b. Geben Sie die Portnummer im Feld "Discover on Port" (Erkennungsport) ein.

   c. Klicken Sie auf "Save" (Speichern).
3. Klicken Sie auf "Refresh" (Aktualisieren). Die Liste der Geräte im lokalen Subnetz wird aktualisiert.

So fügen Sie der Favoritenliste Geräte hinzu:

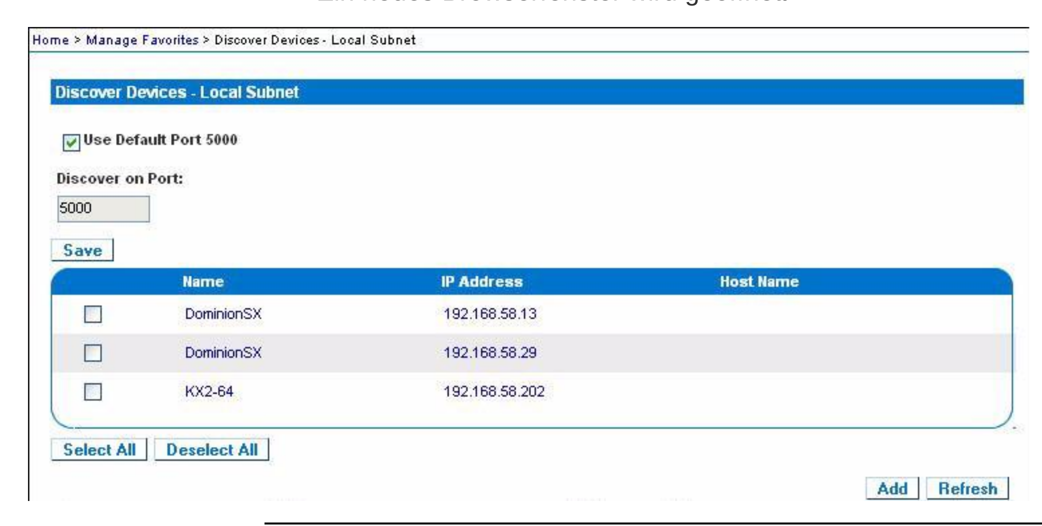
1. Aktivieren Sie das Kontrollkästchen neben dem gewünschten Gerätenamen/der IP-Adresse.
2. Klicken Sie auf "Add" (Hinzufügen).



*Tipp: Verwenden Sie die Schaltflächen **Select All** (Alle auswählen) und **Deselect All** (Alle entfernen), um schnell alle Geräte im Subnetz der Remote-Konsole auszuwählen bzw. diese Auswahl aufzuheben.*

So greifen Sie auf ein erkanntes Gerät zu:

- Klicken Sie auf den Gerätenamen oder die IP-Adresse des Geräts. Ein neues Browserfenster wird geöffnet.

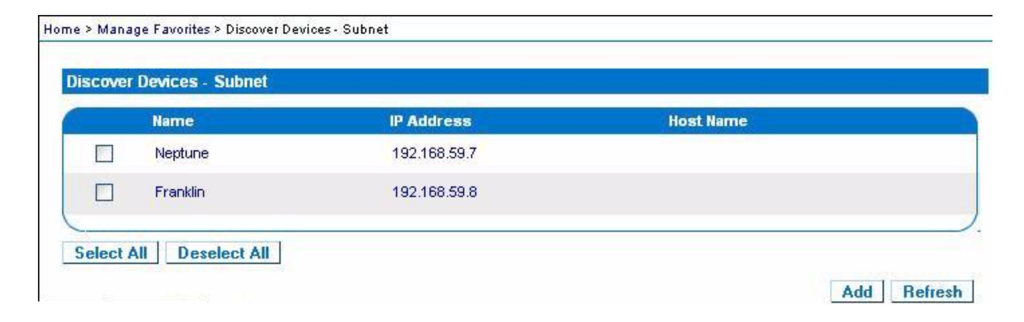


Hinweis: Sowohl IPv4- als auch IPv6-Adressen werden unterstützt.

Erkennen von Geräten auf dem Dominion KX II-Subnetz

Mit dieser Option werden Geräte auf dem Gerätesubnetz erkannt. Dieses ist das Subnetz der Geräte-IP-Adresse von Dominion KX II. Auf die Geräte können Sie direkt von der Subnetzseite aus zugreifen, oder Sie können sie zur Favoritenliste hinzufügen. Siehe***Seite "Favorites List"*** (siehe "***Seite "Favorites List" (Favoritenliste)***" auf Seite 56) (Favoritenliste).

Mit diesem Feature arbeiten mehrere Dominion KX II-Geräte zusammen und werden automatisch skaliert. Die Dominion KX II-Remotekonsole erkennt die Dominion KX II-Geräte und alle sonstigen Raritan-Geräte im Dominion KX II-Subnetz automatisch.



So finden Sie Geräte im Subnetz des Geräts:

1. Wählen Sie Manage > Discover Devices – Dominion KX II Subnet (Verwalten > Geräte erkennen – Dominion KX II-Subnetz) aus. Die Seite "Discover Devices – Dominion KX II Subnet" (Geräte erkennen – Dominion KX II-Subnetz) wird angezeigt.
2. Klicken Sie auf "Refresh" (Aktualisieren). Die Liste der Geräte im lokalen Subnetz wird aktualisiert.

So fügen Sie der Favoritenliste Geräte hinzu:

1. Aktivieren Sie das Kontrollkästchen neben dem gewünschten Gerätenamen/der IP-Adresse.
2. Klicken Sie auf "Add" (Hinzufügen).

---

*Tipp: Verwenden Sie die Schaltflächen **Select All** (Alle auswählen) und **Deselect All** (Alle entfernen), um schnell alle Geräte im Subnetz des Dominion KX II-Geräts auszuwählen bzw. diese Auswahl aufzuheben.*

So greifen Sie auf ein erkanntes Gerät zu:

- Klicken Sie auf den Gerätenamen oder die IP-Adresse des Geräts. Ein neues Browserfenster wird geöffnet.

Hinweis: Sowohl IPv4- als auch IPv6-Adressen werden unterstützt.

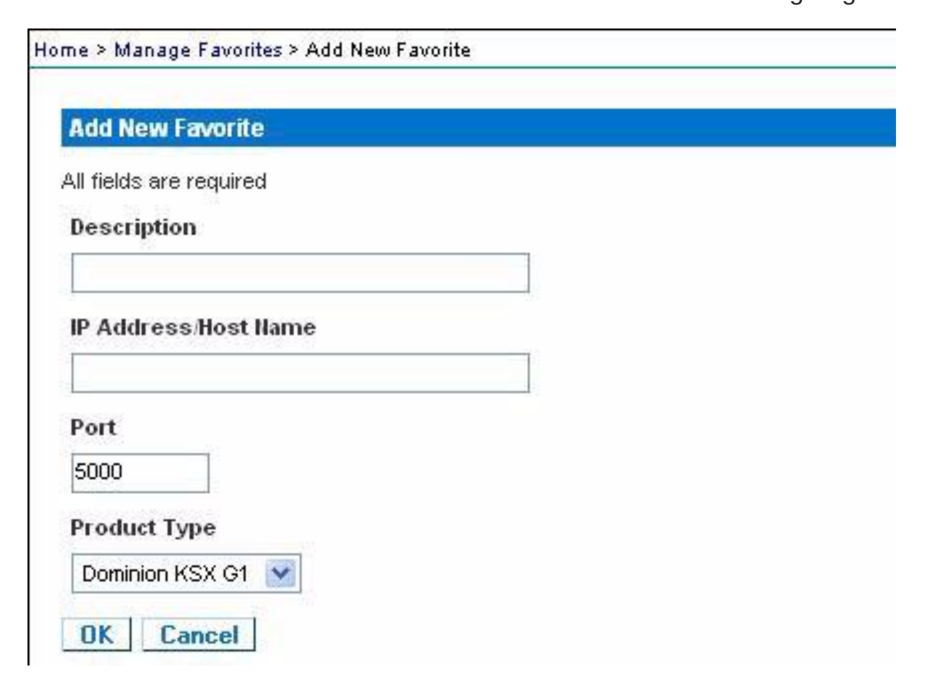
Hinzufügen, Löschen und Bearbeiten der Favoriten

So fügen Sie der Favoritenliste ein Gerät hinzu:

1. Wählen Sie "Manage" > "Add New Device to Favorites" (Verwalten > Neues Gerät zu Favoriten hinzufügen) aus. Die Seite "Add New Favorite" (Neuen Favoriten hinzufügen) wird angezeigt.
2. Geben Sie eine aussagekräftige Beschreibung ein.
3. Geben Sie die IP-Adresse/den Hostnamen des Geräts ein.
4. Ändern Sie ggf. den Erkennungsport.
5. Wählen Sie die Produktart aus.



6. Klicken Sie auf OK. Das Gerät wird Ihrer Favoritenliste hinzugefügt.



So bearbeiten Sie einen Favoriten:

1. Aktivieren Sie auf der Seite "Favorites List" (Favoritenliste) das Kontrollkästchen neben dem gewünschten Dominion KX II-Gerät.
2. Klicken Sie auf die Schaltfläche "Edit" (Bearbeiten). Die Seite "Edit" (Bearbeiten) wird angezeigt.
3. Aktualisieren Sie die Felder nach Bedarf:
   - Beschreibung
   - IP Address/Host Name (IP-Adresse/Hostname) – Geben Sie die IP-Adresse des Dominion KX II-Geräts ein.
   - Port (falls erforderlich)
   - Product Type (Produktart)
4. Klicken Sie auf OK.

So löschen Sie einen Favoriten:

Wichtig: Gehen Sie beim Löschen von Favoriten sorgfältig vor. Sie werden nicht aufgefordert, den Löschvorgang zu bestätigen.

1. Aktivieren Sie das Kontrollkästchen neben dem gewünschten Dominion KX II-Gerät.
2. Klicken Sie auf die Schaltfläche "Delete" (Löschen). Der Favorit wird aus der Favoritenliste entfernt.



Hinweis: Sowohl IPv4- als auch IPv6-Adressen werden unterstützt.

Abmelden

So beenden Sie die Dominion KX II-Remotekonsole:

- Klicken Sie oben rechts auf der Seite auf "Logout" (Abmelden).

Hinweis: Durch das Abmelden werden auch alle geöffneten Sitzungen von Virtual KVM Client und des seriellen Clients geschlossen.

Proxyserverkonfiguration für die Verwendung mit Dominion KX II, MPC, VKC und AKC

Wenn ein Proxyserver verwendet werden muss, muss ein SOCKS-Proxy bereitstehen und auf dem Remote-Client-PC konfiguriert werden.

Hinweis: Wenn der installierte Proxyserver nur das HTTP-Proxyprotokoll unterstützt, können Sie keine Verbindung herstellen.

So konfigurieren Sie den SOCKS-Proxy:

1. Wählen Sie auf dem Client "Control Panel > Internet Options" (Systemsteuerung > Internetoptionen) aus.

a. Klicken Sie auf der Registerkarte "Connections" (Verbindungen) auf "LAN settings" (LAN-Einstellungen). Das Dialogfeld "Local Area Network (LAN) Settings" (LAN-Einstellungen) wird geöffnet.

b. Wählen Sie "Use a proxy server for your LAN" (Proxyserver für LAN verwenden) aus.

c. Klicken Sie auf "Advanced" (Erweitert). Das Dialogfeld "Proxy Settings" (Proxyeinstellungen) wird angezeigt.

d. Konfigurieren Sie die Proxyserver für alle Protokolle. WICHTIG: Wählen Sie nicht "Use the same proxy server for all protocols" (Denselben Proxyserver für alle Protokolle verwenden) aus.

   Hinweis: Der Standardport für ein SOCKS-Proxy (1080) unterscheidet sich vom HTTP-Proxy (3128).

2. Klicken Sie in jedem Dialogfeld auf "OK", um die Einstellungen zu übernehmen.

3. Konfigurieren Sie anschließend die Proxys für die Java™-Applets, indem Sie "Control Panel > Java" (Systemsteuerung > Java) auswählen.



e. Klicken Sie auf der Registerkarte "General" (Allgemein) auf "Network Settings" (Netzwerkeinstellungen). Das Dialogfeld "Network Settings" (Netzwerkeinstellungen) wird angezeigt.

f. Wählen Sie "Use Proxy Server" (Proxyserver verwenden) aus.

g. Klicken Sie auf "Advanced" (Erweitert). Das Dialogfeld "Advanced Network Settings" (Erweiterte Netzwerkeinstellungen) wird angezeigt.

h. Konfigurieren Sie die Proxyserver für alle Protokolle. WICHTIG: Wählen Sie nicht "Use the same proxy server for all protocols" (Denselben Proxyserver für alle Protokolle verwenden) aus.

Hinweis: Der Standardport für ein SOCKS-Proxy (1080) unterscheidet sich vom HTTP-Proxy (3128).

---

4. Wenn Sie ein Standalone-MPC verwenden, müssen Sie folgende Schritte ausführen:

i. Öffnen Sie die Datei "start.bat" im MPC-Verzeichnis in einem Texteditor.

j. Fügen Sie die folgenden Parameter in die Befehlszeile ein. Fügen Sie sie vor "-classpath" ein: -DsocksProxyHost=<socks proxy ip addr> -DsocksProxyPort=<socks proxy port>

   Die Parameter müssen wie folgt aussehen:

```
start javaw -Xmn128M -Xmx512M -XX:MaxHeapFreeRatio=70
-XX:MinHeapFreeRatio=50 -Dsun.java2d.noddraw=true
-DsocksProxyHost=192.168.99.99 -DsocksProxyPort=1080
-classpath .\sdeploy.jar;.\sFoxtrot.jar;.\jaws.jar;.\sMpc.jar
com.raritan.rrc.ui.RRCApplication %1
```

Oberfläche des Multi-Platform-Client

Der Multi-Platform-Client (MPC) von Raritan ist eine grafische Benutzeroberfläche für die Produktlinien von Raritan, mit der Sie Remotezugriff auf Zielserver erhalten, die mit KVM-über-IP-Geräten von Raritan verbunden sind. Informationen zur Verwendung des MPC finden Sie im Benutzerhandbuch **KVM and Serial Access Clients Guide**, das auf der Raritan-Website auf der gleichen Seite wie das Benutzerhandbuch zur Verfügung steht. Dort finden Sie Anweisungen zum Starten des MPC.

Starten des MPC über einen Webbrowser

Wichtig: Unabhängig vom verwendeten Browser müssen Popups für die IP-Adresse des Dominion-Geräts zugelassen werden, damit der MPC geöffnet werden kann.

Wichtig: Nur Mac 10.5 und 10.6 mit einem Intel®-Prozessor können JRE 1.6 ausführen und daher als Client verwendet werden. Mac

10.4.11 und 10.5.8 unterstützen MPC nicht als Standalone-Client.

1. Geben Sie zum Öffnen des MPC von einem Client, auf dem ein beliebiger unterstützter Browser ausgeführt wird, http://IP-ADRESSE/mpc in die Adresszeile ein, wobei "IP-ADRESSE" die IP-Adresse des Raritan-Geräts ist. Der MPC wird in einem neuen Fenster geöffnet.

   Hinweis: Mit dem Befehl "Alt+Tab" können Sie zwischen verschiedenen Fenstern wechseln (nur auf dem lokalen System).

   Wenn sich der MPC öffnet, werden die Raritan-Geräte, die automatisch erkannt und in Ihrem Subnetz gefunden wurden, im Baumformat im Navigator angezeigt.

2. Wenn Ihr Gerät nicht mit Namen im Navigator aufgelistet ist, fügen Sie es manuell hinzu.

   a. Wählen Sie "Connection" > "New Profile" (Verbindung > Neues Profil) aus. Das Fenster "Add Connection" (Verbindung hinzufügen) wird geöffnet.

   b. Geben Sie im Fenster "Add Connection" (Verbindung hinzufügen) eine Gerätebeschreibung ein sowie einen Verbindungstyp an, fügen Sie die IP-Adresse des Geräts hinzu und klicken Sie auf OK. Diese Angaben können Sie später bearbeiten.

3. Doppelklicken Sie im Navigatorfenster auf der linken Seite auf das Symbol für Ihr Raritan-Gerät, um eine Verbindung herzustellen.

Hinweis: Je nach Browser und den Browsersicherheitseinstellungen werden möglicherweise verschiedene Meldungen zur Sicherheit und Zertifikatprüfung sowie Warnungsmeldungen angezeigt. Bestätigen Sie die Optionen, um den MPC zu öffnen.

Hinweis: Wenn Sie Firefox 3.0.3 verwenden, kann es zu Problemen beim Starten der Anwendung kommen. Wenn dies der Fall ist, löschen Sie den Browser-Cache und starten Sie die Anwendung erneut.



Virtual KVM Client

Überblick

Wenn Sie über die Remotekonsole auf einen Zielserver zugreifen, wird ein Fenster für den Virtual KVM Client (VKC) geöffnet. Es steht ein Virtual KVM Client für jeden verbundenen Zielserver zur Verfügung. Auf diese Fenster kann über die Windows®-Taskleiste zugegriffen werden.

Die Fenster des Virtual KVM Client können minimiert, maximiert und auf dem Desktop verschoben werden.

Hinweis: Beachten Sie, dass beim Aktualisieren des HTML-Browsers die Verbindung des Virtual KVM Client beendet wird.

Hinweis: Wenn Sie Firefox 3.0.3 verwenden, kann es zu Problemen beim Starten der Anwendung kommen. Wenn dies der Fall ist, löschen Sie den Browser-Cache und starten Sie die Anwendung erneut.

Verbinden mit einem KVM-Zielserver

So stellen Sie eine Verbindung mit einem KVM-Zielserver her:

1. Klicken Sie in der Dominion KX II-Remotekonsole auf die Registerkarte "Port Access" (Portzugriff). Die Seite "Port Access" (Portzugriff) wird angezeigt.
2. Klicken Sie auf den Portnamen des Zielgeräts, auf das Sie zugreifen möchten. Das Menü "Port Action" (Portaktion) wird angezeigt.
3. Klicken Sie auf "Connect" (Verbinden). Ein Fenster des ***Virtual KVM Client*** (auf Seite 63) wird für den mit dem betreffenden Port verbundenen Zielserver geöffnet.

VKC-Symbolleiste

Hinweis: Die KX II-101 VKC Schnittstelle unterscheidet sich von den anderen Dominion KX-Produkten. Siehe VKC Toolbar for the KX II-101.

Schaltfläche	Schaltflächenname	Beschreibung
	Verbindungseigenschaften	Öffnet das Dialogfeld "Modify Connection Properties" (Verbindungseigenschaften bearbeiten), über das Sie die Bandbreitenoptionen (z. B. Verbindungsgeschwindigkeit, Farbtiefe usw.) manuell anpassen können.
	Video Settings	Öffnet das Dialogfeld "Video Settings" (Videoeinstellungen), über das Sie die



Schaltfläche	Schaltflächenname	Beschreibung
	(Videoeinstellungen)	Videokonvertierungsparameter manuell anpassen können.
	Color Calibration (Farbkalibrierung)	Dient zum Anpassen der Farbeinstellungen, um überflüssiges Farbrauschen zu reduzieren. Diese Option ist identisch mit der Auswahl von "Video" > "Color Calibrate" (Video > Farbkalibrierung).
	Target Screenshot (Screenshot des Zielgeräts)	Klicken Sie auf diese Option, um einen Screenshot des Zielservers aufzunehmen und diesen in einer Datei Ihrer Wahl zu speichern.
	Synchronize Mouse (Maus synchronisieren)	Erzwingt im Zwei-Cursor-Modus die erneute Ausrichtung des Zielservercursors mit dem Cursor.
	Refresh Screen (Anzeige aktualisieren)	Aktualisiert den Videobildschirm.
	Auto-sense Video Settings (Videoeinstellungen automatisch erkennen)	Aktualisiert die Videoeinstellungen (Auflösung, Aktualisierungsfrequenz).
	"Smart Card"	Öffnet ein Dialogfeld, in dem Sie aus einer Liste von Smart Card-Lesegeräten, die an einen Client-PC angeschlossen sind, auswählen können. *Hinweis: Diese Funktion ist nur für den KX II 2.1.10 oder höher verfügbar.*
	Send Ctrl+Alt+Delete (Strg+Alt+Entf senden)	Sendet die Tastenkombination "Strg+Alt+Entf" an den Zielserver.



Schaltfläche	Schaltflächenname	Beschreibung
	Single Cursor Mode (Ein-Cursor-Modus)	Startet den Ein-Cursor-Modus, bei dem der lokale Cursor nicht mehr auf dem Bildschirm angezeigt wird. Drücken Sie Strg+Alt+O, um diesen Modus zu beenden. Alternativ dazu können Sie "Single/Double Cursor" (Ein/Zwei Cursor) im Kontextmenü auswählen, das über die Tastenkombination Ctrl+Alt+M geöffnet wird.
	Vollbildmodus	Maximiert die Anzeige des Zielserverdesktops, sodass er auf dem gesamten Bildschirm angezeigt wird.
	"Scaling" Skalieren	Vergrößert oder verkleinert die Zielvideogröße, sodass Sie den gesamten Inhalt des Zielserverfensters anzeigen können, ohne die Bildlaufleiste verwenden zu müssen.

Wechseln zwischen KVM-Zielservern

Über Dominion KX II können Sie auf mehrere KVM-Zielserver zugreifen. Dominion KX II ermöglicht das Wechseln zwischen verschiedenen Zielservern.

Hinweis: Dieses Feature ist nur in der Dominion KX II-Remotekonsole verfügbar.

So wechseln Sie zwischen KVM-Zielservern:

1. Rufen Sie die Dominion KX II-Seite "Port Access" (Portzugriff) auf, während bereits auf einen Zielserver zugegriffen wird.
2. Klicken Sie auf den Portnamen des Zielgeräts, auf das Sie zugreifen möchten. Das Menü "Port Action" (Portaktion) wird angezeigt.
3. Wählen Sie im Menü "Port Action" (Portaktion) die Option "Switch From" (Wechseln von) aus. Das Fenster des Virtual KVM Clients wechselt zu dem von Ihnen gewählten Zielserver.

Stromzufuhrsteuerung eines Zielservers

Hinweis: Diese Features stehen nur zur Verfügung, wenn Sie Stromzuordnungen vorgenommen haben.

So schalten Sie einen KVM-Zielserver aus und wieder ein:

1. Klicken Sie in der Dominion KX II-Remotekonsole auf die Registerkarte "Port Access" (Portzugriff). Die Seite "Port Access" (Portzugriff) wird angezeigt.
2. Klicken Sie unter "Port Name" (Portname) auf den entsprechenden Zielserver. Das Menü "Port Action" (Portaktion) wird angezeigt.
3. Wählen Sie "Power Cycle" (Aus- und Einschalten) aus. Eine Bestätigungsmeldung wird angezeigt.

So schalten Sie einen Zielserver ein:

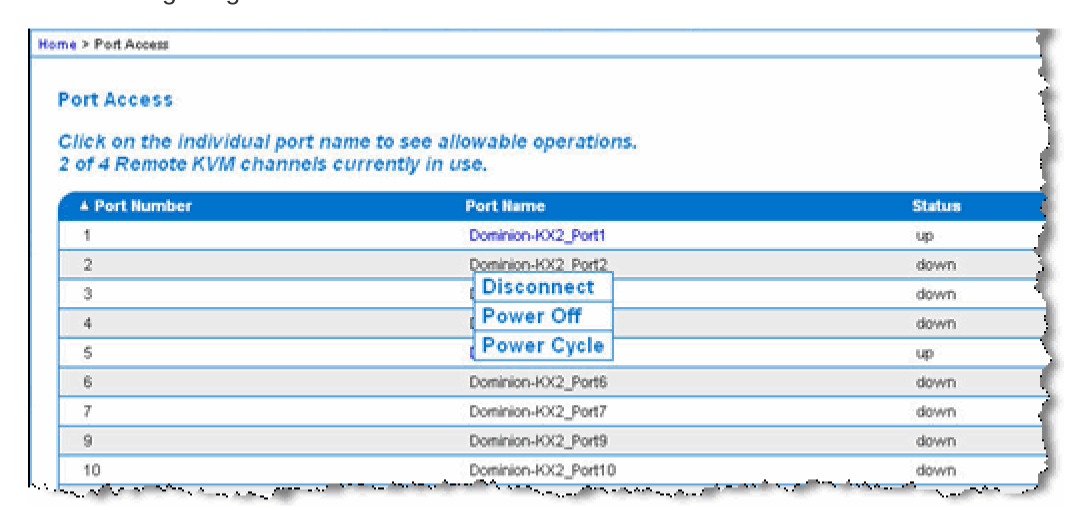
1. Klicken Sie in der Dominion KX II-Remotekonsole auf die Registerkarte "Port Access" (Portzugriff). Die Seite "Port Access" (Portzugriff) wird angezeigt.
2. Klicken Sie unter "Port Name" (Portname) auf den entsprechenden Zielserver. Das Menü "Port Action" (Portaktion) wird angezeigt.
3. Wählen Sie "Power On" (Strom ein) aus. Eine Bestätigungsmeldung wird angezeigt.

So schalten Sie einen Zielserver aus:

1. Klicken Sie in der Dominion KX II-Remotekonsole auf die Registerkarte "Port Access" (Portzugriff). Die Seite "Port Access" (Portzugriff) wird angezeigt.
2. Klicken Sie unter "Port Name" (Portname) auf den entsprechenden Zielserver. Das Menü "Port Action" (Portaktion) wird angezeigt.



3. Wählen Sie "Power Off" (Strom aus) aus. Eine Bestätigungsmeldung wird angezeigt.



Trennen von KVM-Zielservern

Hinweis: Diese Option steht auf der lokalen Dominion KX II-Konsole nicht zur Verfügung. Sie können die Verbindung zum gewechselten Zielgerät auf der lokalen Konsole nur trennen, indem Sie die Zugriffstaste verwenden.

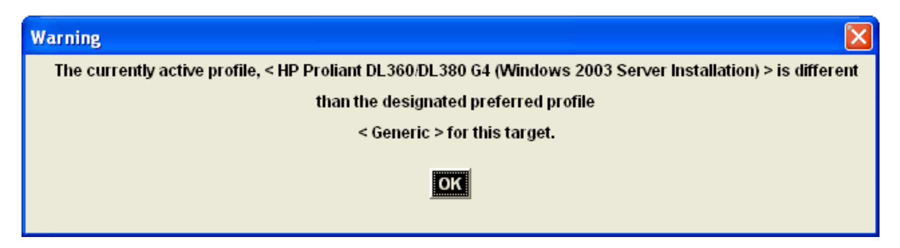
So trennen Sie einen Zielserver:

1. Klicken Sie auf den Portnamen des Zielgeräts, das Sie trennen möchten. Das Menü "Port Action" (Portaktion) wird angezeigt.
2. Wählen Sie "Disconnect" (Trennen) aus.

Tipp: Sie können das Fenster des Virtual KVM Client auch schließen, indem Sie im Virtual KVM-Menü die Option "Connection" > "Exit" (Verbindung > Beenden) auswählen.

Auswählen von USB-Profilen

Wenn Sie zum ersten Mal eine Verbindung zu einem KVM-Zielserver herstellen, wie unter ***Verbinden mit einem KVM-Zielserver*** (auf Seite 63) beschrieben, wird automatisch das für den Port bevorzugte USB-Profil verwendet. Wenn Sie zuvor bereits über ein anderes Profil eine Verbindung zum Zielserver hergestellt haben, wird das USB-Profil der letzten Verbindung verwendet. Sie werden auf die Verwendung eines Profils, das nicht dem bevorzugten Profil entspricht, aufmerksam gemacht, indem eine Warnmeldung ähnlich der im folgenden Beispiel dargestellten Meldung angezeigt wird.



Nachdem Sie eine Verbindung zu einem Zielserver hergestellt haben, können Sie das USB-Profil ggf. ändern. Standardmäßig werden die Profile im USB-Profilmenü im VKC angezeigt, die Sie am wahrscheinlichsten verwenden. Diese Profile wurden vom Administrator für die Verwendung mit dem verbundenen Zielserver voreingestellt, basierend auf Ihren betrieblichen Anforderungen. Über die Option "Other Profiles" (Weitere Profile) im USB-Profilmenü stehen jedoch alle Profile zur Auswahl zur Verfügung.

▶ So wählen Sie ein USB-Profil aus:

1. Stellen Sie eine Verbindung zu einem KVM-Zielserver, wie unter ***Verbinden mit einem KVM-Zielserver*** (auf Seite 63) beschrieben, her.
2. Wählen Sie im VKC ein USB-Profil aus dem USB-Profilmenü aus.

   Der Name des Profils gibt das Betriebssystem oder den Server an, mit dem es verwendet werden sollte. Weitere Informationen zu USB-Profilen finden Sie unter ***USB-Profile*** (auf Seite 118).



Verbindungseigenschaften

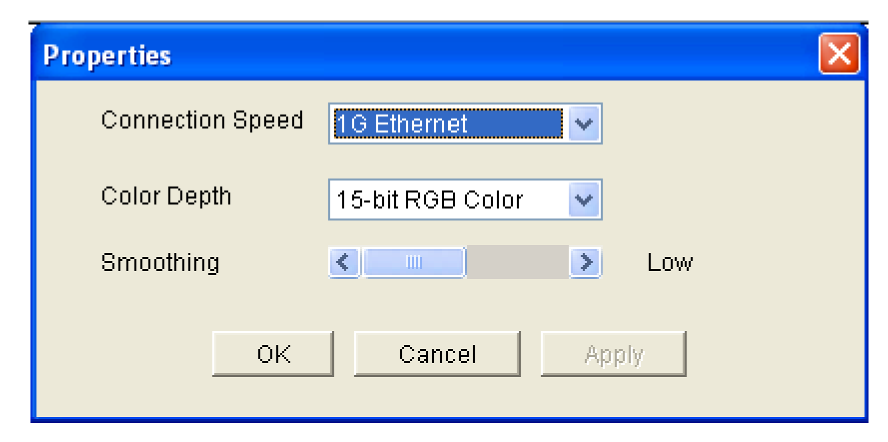
Die dynamischen Videokomprimierungsalgorithmen gewährleisten die Verwendbarkeit der KVM-Konsole unter variierenden Bandbreitenbeschränkungen. Die Geräte optimieren die KVM-Ausgabe nicht nur für LAN-, sondern auch für WAN-Verbindungen. Diese Geräte können zudem die Farbtiefe steuern und die Videoausgabe beschränken, um für jede Bandbreite ein optimales Gleichgewicht zwischen Videoqualität und Systemreaktion bereitzustellen.

Sie können die Parameter im Dialogfeld "Properties" (Eigenschaften) Ihren Anforderungen für unterschiedliche Betriebsumgebungen anpassen. Einmal vorgenommene und gespeicherte Verbindungseigenschaften werden auch für spätere Verbindungen zu Geräten der 2. Generation gespeichert.

Hinweis: Der VKC für den KX II-101 verwendet Symbole, die sich von den Symbolen, die im VKC für andere Dominion KX-Produkte unterscheiden. Weitere Informationen finden Sie unter VKC Toolbar for the KX II-101.

So legen Sie die Verbindungseigenschaften fest:

1. Wählen Sie "Connection" > "Properties" (Verbindung > Eigenschaften) oder klicken Sie auf die Schaltfläche "Connection Properties" (Verbindungseigenschaften) in der Symbolleiste. Das Dialogfeld "Properties" (Eigenschaften) wird angezeigt.



Hinweis: 1G Ethernet wird vom KX II-101 nicht unterstützt.

Hinweis: Der VKC für den KX II-101 verwendet Symbole, die sich von den Symbolen, die im VKC für andere Dominion KX-Produkte unterscheiden. Weitere Informationen finden Sie unter VKC Toolbar for the KX II-101.



2. Wählen Sie in der Dropdownliste "Connection Speed" (Verbindungsgeschwindigkeit) die gewünschte Verbindungsgeschwindigkeit aus. Das Gerät kann die verfügbare Bandbreite automatisch erkennen und die Bandbreitenverwendung nicht beschränken. Sie können diese Verwendung jedoch auch gemäß den Bandbreitenbeschränkungen anpassen.
   - Automatisch
   - 1G Ethernet
   - 100 MB Ethernet
   - 10 MB Ethernet
   - 1,5 MB (MAX DSL/T1)
   - 1 MB (Schnelles DSL/T1)
   - 512 KB (Mittleres DSL/T1)
   - 384 KB (Langsames DSL/T1)
   - 256 KB (Kabel)
   - 128 KB (Dual-ISDN)
   - 56 KB (ISP-Modem)
   - 33 KB (Schnelles Modem)
   - 24 KB (Langsames Modem)

   Diese Einstellungen sind nicht als genaue Geschwindigkeitsangaben zu verstehen, sondern als Optimierungen für bestimmte Bedingungen. Der Client und der Server versuchen stets, Videodaten so schnell wie möglich über das Netzwerk zu übertragen, unabhängig von der aktuellen Netzwerkgeschwindigkeit und Codierungseinstellung. Das System arbeitet jedoch am schnellsten, wenn die Einstellungen der tatsächlichen Umgebung entsprechen.
3. Wählen Sie in der Dropdownliste "Color Depth" (Farbtiefe) die gewünschte Farbtiefe aus. Das Gerät kann die an Remotebenutzer übertragene Farbtiefe dynamisch anpassen, um die Verwendbarkeit in allen Bandbreiten zu maximieren.
   - 15-Bit-Farbe (RGB)
   - 8-Bit-Farbe (RGB)
   - 4-Bit-Farbe
   - 4-Bit-Graustufen
   - 3-Bit-Graustufen
   - 2-Bit-Graustufen
   - Schwarzweiß



Wichtig: Für die meisten Verwaltungsaufgaben (Überwachung, erneute Konfiguration von Servern usw.) wird das von den modernen Videografikkarten bereitgestellte vollständige 24-Bit- oder 32-Bit-Farbspektrum nicht benötigt. Durch den Versuch, solch hohe Farbtiefen zu übertragen, wird Netzwerkbandbreite verschwendet.

4. Verwenden Sie den Schieberegler um die gewünschte Glättung auszuwählen (nur im 15-Bit-Farbmodus). Die Glättungsebene bestimmt, wie stark Bildschirmbereiche mit geringer Farbvariation zu einer einheitlichen Farbe zusammengefasst werden. Die Glättung verbessert das Aussehen des Zielgerätbildes, da dadurch das Videorauschen verringert wird.
5. Klicken Sie auf OK, um die Eigenschaften festzulegen.

Verbindungsinformationen

So erhalten Sie Informationen über die Verbindung des Virtual KVM Client:

- Wählen Sie "Connection" > "Connection Info" (Verbindung > Verbindungsinformationen) aus. Das Fenster "Connection Info" (Verbindungsinformationen) wird angezeigt.

Zur aktuellen Verbindung werden folgende Informationen angezeigt:

- Device Name (Gerätename) – Der Name des Geräts.
- IP-Address (IP-Adresse) – Die IP-Adresse des Geräts.
- Port – Der TCP/IP-Port für die KVM-Kommunikation, über den auf das Zielgerät zugegriffen wird.
- Data In/Second (Dateneingang/Sekunde) – Eingehende Datenrate.
- Data Out/Second (Datenausgang/Sekunde) – Ausgehende Datenrate.
- Connect Time (Verbindungsdauer) – Die Dauer der Verbindung.
- FPS – Frames pro Sekunde der übertragenen Videobilder.
- Horizontal Resolution (Horizontale Auflösung) – Die horizontale Bildschirmauflösung.
- Vertical Resolution (Vertikale Auflösung) – Die vertikale Bildschirmauflösung.
- Refresh Rate (Aktualisierungfrequenz) – Gibt an, wie häufig die Anzeige aktualisiert wird.
- Protocol Version (Protokollversion) – Die RFB-Protokollversion.

So kopieren Sie diese Informationen:

- Klicken Sie auf "Copy to Clipboard" (In Zwischenablage kopieren). Anschließend können die Informationen in ein Programm Ihrer Wahl eingefügt werden.

Tastaturoptionen

Tastaturmakros

Tastaturmakros gewährleisten, dass für den Zielserver vorgesehene Tastenkombinationen an den Zielserver gesendet und nur von diesem interpretiert werden. Andernfalls werden sie von dem Computer interpretiert, auf dem der Virtual KVM Client ausgeführt wird (Client-PC).

Makros werden auf dem Client-PC gespeichert und sind PC-spezifisch. Wenn Sie einen anderen PC verwenden, sehen Sie daher Ihre Makros nicht. Wenn eine andere Person Ihren PC verwendet und sich mit einem anderen Benutzernamen anmeldet, werden ihr die Makros angezeigt, da sie für den gesamten Computer gelten.

Im Virtual KVM Client erstellte Tastaturmakros stehen im MPC zur Verfügung und umgekehrt. Tastaturmakros, die auf dem AKC erstellt wurden, können jedoch nicht in VKC oder MPC verwendet werden. Dies trifft umgekehrt ebenfalls zu.

Erstellen eines Tastaturmakros

► **So erstellen Sie ein Makro:**

1. Klicken Sie auf "Keyboard" > "Keyboard Macros" (Tastatur > Tastaturmakros). Das Dialogfeld "Keyboard Macros" (Tastaturmakros) wird angezeigt.
2. Klicken Sie auf "Add" (Hinzufügen". Das Dialogfeld "Add Keyboard Macro" (Tastaturmakro hinzufügen) wird angezeigt.
3. Geben Sie im Feld "Keyboard Macro Name" (Name des Tastaturmakros) einen Namen für das Makro ein. Dieser Name wird nach der Erstellung im Tastaturmenü angezeigt.
4. Wählen Sie in der Dropdownliste im Feld "Hot-Key Combination" (Zugriffstastenkombination) eine Tastenkombination aus. Dies ermöglicht es Ihnen, das Makro mit einer vordefinierten Tastenkombination auszuführen. **Optional**
5. Wählen Sie in der Dropdownliste "Keys to Press" (Zu betätigende Tasten) alle Tasten aus, die Sie verwenden möchten, um die Tastenkombination zu emulieren, die zum Ausführen des Befehls verwendet wird. Wählen Sie die Tasten in der Reihenfolge aus, in der sie betätigt werden sollen. Wählen Sie nach jeder gewählten Taste "Add Key" (Taste hinzufügen) aus. Nach der Auswahl jeder Taste wird diese im Feld "Macro Sequence" (Makrosequenz) angezeigt und ein Befehl zum Freigeben der Taste wird automatisch hinzugefügt.



6. Um die Funktion "Send Text to Target" (Text an Ziel senden) für das Makro zu verwenden, klicken Sie auf die Schaltfläche "Construct Macro from Text" (Makro aus Text erstellen).
7. Erstellen Sie beispielsweise ein Makro zum Schließen eines Fensters durch die Tastenkombination "Linke Strg-Taste+Esc". Dieses wird im Feld "Macro Sequenz" (Makrosequenz) wie folgt angezeigt:

   Linke Strg-Taste drücken

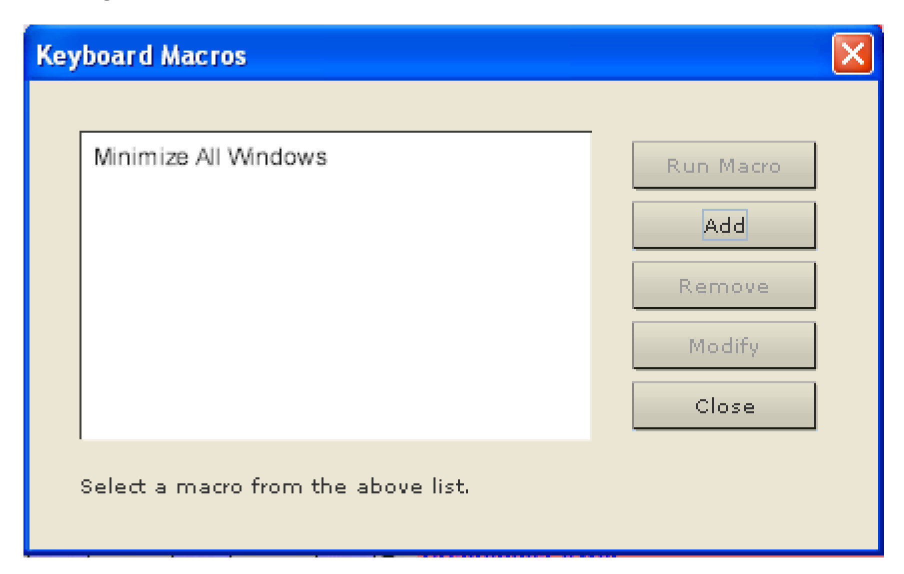
   Linke Strg-Taste freigeben

   Esc drücken

   Esc freigeben

8. Überprüfen Sie das Feld "Macro Sequence" (Makrosequenz), um sicherzustellen, dass die Makrosequenz korrekt definiert wurde.
   a. Wenn Sie einen Schritt aus der Sequenz entfernen möchten, markieren Sie diesen, und klicken Sie auf "Remove" (Entfernen).
   b. Wenn Sie die Reihenfolge der Schritte in der Sequenz ändern möchten, klicken Sie auf den Schritt und anschließend auf die Pfeil-nach-oben- oder Pfeil-nach-unten-Taste um die Position des Schritts wie gewünscht zu ändern.
9. Klicken Sie zum Speichern des Makros auf OK. Klicken Sie auf "Clear" (Löschen), um alle Felder zu löschen und erneut mit der Auswahl zu beginnen. Wenn Sie auf OK klicken, wird das Dialogfenster "Keyboard Macros" (Tastaturmakros) mit dem neuen Tastaturmakro angezeigt.

10. Klicken Sie im Dialogfeld "Keyboard Macros" (Tastaturmakros) auf "Close" (Schließen). Das Makro wird nun im Tastaturmenü der Anwendung angezeigt. Wählen Sie das neue Makro im Menü aus, um es auszuführen, oder verwenden Sie die dem Makro zugeordnete Tastenkombination.



Ausführen eines Tastaturmakros

Wenn Sie ein Tastaturmakro erstellt haben, können Sie es über das zugeordnete Tastaturmakro ausführen oder es aus dem Tastaturmenü auswählen.

Ausführen eines Makros über die Menüleiste

Ein erstelltes Makro wird im Menü "Keyboard" (Tastatur) angezeigt. Führen Sie das Tastaturmakro aus, indem Sie im Menü "Keyboard" (Tastatur) auf das Makro klicken.

Ausführen eines Makros mithilfe einer Tastaturkombination

Wenn Sie beim Erstellen eines Makros eine Tastenkombination zugewiesen haben, können Sie das Makro durch Drücken der entsprechenden Tasten ausführen. Drücken Sie beispielsweise gleichzeitig die Tasten Strg+Alt+0, um alle Fenster auf einem Windows-Zielserver zu minimieren.

Bearbeiten und Löschen von Tastaturmakros

► **So ändern Sie ein Makro:**

1. Wählen Sie **Keyboard > Keyboard Macros** (Tastatur > Tastaturmakros). Das Dialogfeld "Keyboard Macros" (Tastaturmakros) wird angezeigt.



2. Wählen Sie das gewünschte Makro aus der Liste aus.
3. Klicken Sie auf **Modify** (Ändern). Das Dialogfeld **Add/Edit Macro** (Makro hinzufügen/bearbeiten) wird angezeigt.
4. Nehmen Sie die gewünschten Änderungen vor.
5. Klicken Sie auf OK.

So entfernen Sie ein Makro:

1. Wählen Sie **Keyboard > Keyboard Macros** (Tastatur > Tastaturmakros). Das Dialogfeld "Keyboard Macros" (Tastaturmakros) wird angezeigt.
2. Wählen Sie das gewünschte Makro aus der Liste aus.
3. Klicken Sie auf "Remove" (Entfernen). Das Makro wird gelöscht.

Tastenkombinationen, die sich mit Blade-Chassis-Tastenfolgen überschneiden, werden nicht an die Blades in diesem Chassis gesendet.

Einstellungen für CIM-Tastatur/Mausoptionen

So greifen Sie auf das DCIM-USBG2-Setupmenü zu:

1. Klicken Sie mit der Maus in ein Fenster, wie z. B. Windows-Editor (Windows®-Betriebssystem) o. Ä.
2. Wählen Sie die Optionen für "Set CIM Keyboard/Mouse options" (CIM-Tastatur/-Maus festlegen) aus. Dies ist das Äquivalent für das Senden von linke Strg-Taste und Num Lock an das Ziel. Die Optionen für das CIM-Setupmenü werden angezeigt.
3. Legen Sie die Sprache und Mauseinstellungen fest.
4. Verlassen Sie das Menü, um zur normalen CIM-Funktionalität zurückzukehren.

Videoeigenschaften

Refresh Screen (Anzeige aktualisieren)

Der Befehl "Refresh Screen" (Anzeige aktualisieren) erzwingt eine Aktualisierung des Videobildschirms. Videoeinstellungen können auf verschiedene Art und Weise automatisch aktualisiert werden:

- Der Befehl "Refresh Screen" (Anzeige aktualisieren) erzwingt eine Aktualisierung des Videobildschirms.
- Mit dem Befehl "Auto-sense Video Settings" (Videoeinstellungen automatisch erkennen) werden die Videoeinstellungen des Zielservers automatisch erkannt.
- Mit dem Befehl "Calibrate Color" (Farbe kalibrieren) wird das Videobild kalibriert, um die angezeigten Farben zu verbessern.

Darüber hinaus können Sie die Einstellungen manuell über den Befehl "Video Settings" (Videoeinstellungen) anpassen.

Hinweis: Der VKC für den KX II-101 verwendet Symbole, die sich von den Symbolen, die im VKC für andere Dominion KX-Produkte unterscheiden. Weitere Informationen finden Sie unter VKC Toolbar for the KX II-101.

Führen Sie einen der folgenden Schritte aus, um die Videoeinstellungen zu aktualisieren:

- Wählen Sie "Video" > "Refresh Screen" (Video > Anzeige aktualisieren) aus oder klicken Sie auf die Schaltfläche "Refresh Screen" (Anzeige aktualisieren) in der Symbolleiste.



Automatisches Erkennen der Videoeinstellungen

Der Befehl "Auto-sense Video Settings" (Videoeinstellungen automatisch erkennen) erzwingt das erneute Erkennen der Videoeinstellungen (Auflösung, Aktualisierungsfrequenz) und erstellt die Videoanzeige neu.

Hinweis: Der VKC für den KX II-101 verwendet Symbole, die sich von den Symbolen, die im VKC für andere Dominion KX-Produkte unterscheiden. Weitere Informationen finden Sie unter VKC Toolbar for the KX II-101.

Führen Sie zur automatischen Erkennung der Videoeinstellungen die folgenden Schritte aus:

- Wählen Sie "Video" > "Auto-sense Video Settings" (Video > Videoeinstellungen automatisch erkennen) aus oder klicken Sie auf die Schaltfläche "Auto-Sense Video Settings" (Videoeinstellungen automatisch erkennen) in der Symbolleiste. Eine Meldung mit der Information, dass die automatische Anpassung läuft, wird angezeigt.

Kalibrieren der Farben

Verwenden Sie den Befehl "Calibrate Color" (Farbe kalibrieren), um die Farbstufen (Farbton, Helligkeit, Sättigung) der übertragenen Videobilder zu optimieren. Die Farbeinstellungen basieren auf dem jeweiligen Zielserver.

Hinweis: Der Befehl "Calibrate Color" (Farbe kalibrieren) gilt nur für die aktuelle Verbindung.

Hinweis: Das Modell KX II-101 unterstützt die Kalibrierung der Farben.

Um die Farbe zu kalibrieren, führen Sie Folgendes durch:

- Wählen Sie "Video" > "Calibrate Color" (Video > Farbe kalibrieren) oder klicken Sie auf die Schaltfläche "Calibrate Color" (Farbe kalibrieren) in der Symbolleiste. Die Farbkalibrierung des Zielgerätebildschirms wird aktualisiert.

Konfigurieren von Videoeinstellungen

Verwenden Sie den Befehl "Video Settings" (Videoeinstellungen), um die Videoeinstellungen manuell anzupassen.

So ändern Sie die Videoeinstellungen:

1. Wählen Sie "Video" > "Video Settings" (Video > Videoeinstellungen) aus oder klicken Sie auf die Schaltfläche "Video Settings" (Videoeinstellungen) in der Symbolleiste, um das Dialogfeld "Video Settings" (Videoeinstellungen) zu öffnen.
2. Passen Sie die folgenden Einstellungen nach Wunsch an. Wenn Sie die Einstellungen anpassen, sind die Änderungen sofort sichtbar:
   a. Noise Filter (Rauschfilter)

      Das Gerät kann elektrische Störungen aus der Videoausgabe von Grafikkarten herausfiltern. Dieses Feature optimiert die Bildqualität und reduziert die Bandbreite. Höhere Einstellungen übermitteln nur dann Variantenpixel, wenn bei einem Vergleich mit den Nachbarpixeln eine starke Farbabweichung vorliegt. Eine zu hohe Einstellung des Grenzwerts kann jedoch zu einer unbeabsichtigten Filterung von gewünschten Bildschirmänderungen führen.
      Niedrigere Einstellungen übermitteln die meisten Pixeländerungen. Eine zu niedrige Einstellung dieses Grenzwerts kann zu einer höheren Bandbreitenverwendung führen.

   b. PLL Settings (PLL-Einstellungen)

      Clock (Uhr) – Diese Option steuert, wie schnell Videopixel auf dem Videobildschirm angezeigt werden. Änderungen an den Uhreinstellungen führen zu einer horizontalen Streckung oder Stauchung des Videobilds. Als Einstellung werden ungerade Zahlen empfohlen. Üblicherweise sollte diese Einstellung nicht geändert werden, da die automatische Erkennung meist korrekt ist.

      Phase – Die Phasenwerte liegen zwischen 0 und 31 und werden zyklisch durchlaufen. Halten Sie bei dem Phasenwert an, der das beste Videobild für den aktiven Zielserver ergibt.

   c. Brightness (Helligkeit): Mithilfe dieser Einstellung passen Sie die Helligkeit der Zielserveranzeige an.

   d. Brightness Red (Helligkeit – Rot) – Steuert die Helligkeit der Anzeige des Zielservers für das rote Signal.

   e. Brightness Green (Helligkeit – Grün) – Steuert die Helligkeit des grünen Signals.

   f. Brightness Blue (Helligkeit – Blau) – Steuert die Helligkeit des blauen Signals.



g. Contrast Red (Kontrast – Rot) – Steuert den Kontrast des roten Signals.

h. Contrast Green (Kontrast – Grün) – Steuert das grüne Signal.

i. Contrast Blue (Kontrast – Blau) – Steuert das blaue Signal.

Wenn das Videobild extrem verschwommen oder unscharf wirkt, können die Einstellungen für die Uhr und die Phase so gewählt werden, dass auf dem aktiven Zielserver ein besseres Bild angezeigt wird.

Warnung: Gehen Sie beim Ändern der Einstellungen für die Uhr und die Phase sorgfältig vor. Änderungen können zu Verzerrungen oder sogar zum Verlust des Videobildes führen, und Sie können möglicherweise die vorherigen Einstellungen nicht wiederherstellen. Wenden Sie sich an den technischen Kundendienst von Raritan, bevor Sie Änderungen vornehmen.

---

j. Horizontal Offset (Horizontaloffset) – Steuert die horizontale Positionierung der Zielserveranzeige auf dem Bildschirm.

k. Vertical Offset (Vertikaloffset) – Steuert die vertikale Positionierung der Zielserveranzeige auf dem Bildschirm.

3. Wählen Sie "Automatic Color Calibration" (Automatische Farbkalibrierung) aus, um diese Funktion zu aktivieren.

4. Wählen Sie den Videoerkennungsmodus aus:

   - Best possible video mode (Bestmöglicher Videomodus)

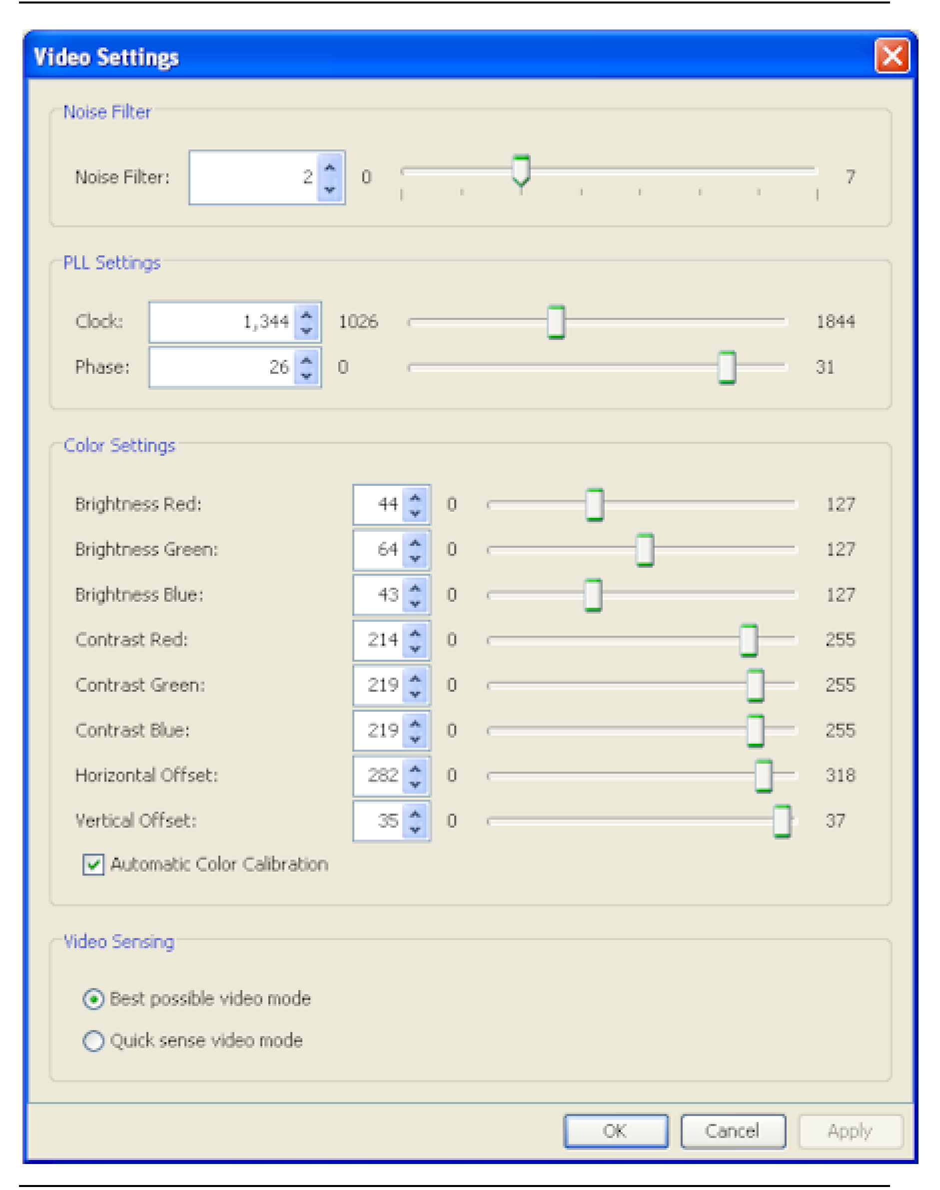
   Beim Wechseln von Zielgeräten oder Zielauflösungen führt das Gerät die vollständige automatische Erkennung durch. Bei dieser Option wird das Videobild so kalibriert, dass die bestmögliche Bildqualität erzielt wird.

   - Quick sense video mode (Videomodus schnell erkennen)

   Bei dieser Option führt das Gerät eine schnelle automatische Erkennung des Videomodus durch, um das Bild des Zielgeräts schneller anzuzeigen. Diese Option eignet sich insbesondere für die Eingabe der BIOS-Konfiguration eines Zielservers nach einem Neustart.

5. Klicken Sie auf OK, um die Einstellungen zu übernehmen, und schließen Sie das Dialogfenster. Klicken Sie auf "Apply" (Übernehmen), um die Einstellungen zu übernehmen, ohne das Dialogfenster zu schließen.

Hinweis: Einige Sun-Hintergrundanzeigen (z. B. Anzeigen mit sehr dunklen Rändern) werden auf bestimmten Sun-Servern nicht exakt zentriert abgebildet. Verwenden Sie einen anderen Hintergrund, oder platzieren Sie auf der Anzeige oben links ein helleres Symbol.



Hinweis: Der VKC für den KX II-101 verwendet Symbole, die sich von den Symbolen, die im VKC für andere Dominion KX-Produkte unterscheiden. Weitere Informationen finden Sie unter VKC Toolbar for the KX II-101.



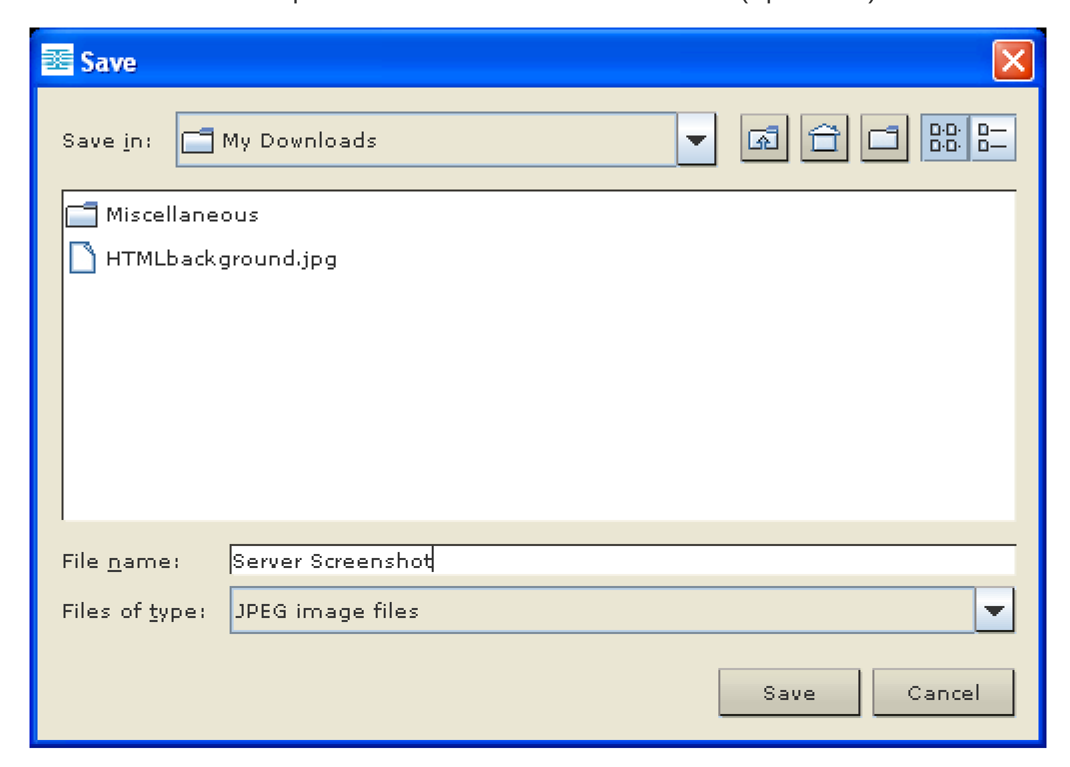
Verwenden der Funktion "Screenshot from Target" (Screenshot vom Zielgerät)

Mit dem Befehl "Screenshot from Target" (Screenshot vom Zielgerät) können Sie einen Screenshot vom Zielserver aufnehmen. Sie können diesen Screenshot anschließend an einem Speicherort Ihrer Wahl als Bitmap-, JPEG- oder PNG-Datei speichern.

Hinweis: Die Funktion "Screenshot from Target" (Screenshot vom Zielgerät) ist für das Modell KX II-101 nicht verfügbar.

So nehmen Sie einen Screenshot vom Zielserver auf:

1. Wählen Sie "Video" > "Screenshot from Target" (Video > Screenshot vom Zielgerät) aus oder klicken Sie auf die Schaltfläche "Screenshot from Target" (Screenshot vom Zielgerät) in der Symbolleiste.
2. Wählen Sie im Dialogfenster "Save" (Speichern) den Speicherort für die Datei aus, benennen Sie sie und wählen Sie ein Dateiformat aus der Dropdownliste "Files of Type" (Dateitypen) aus.
3. Klicken Sie zum Speichern des Screenshots auf "Save" (Speichern).



Ändern der höchsten Aktualisierungsrate

Wenn die von Ihnen verwendete Videokarte kundenspezifische Software verwendet und Sie über MPC oder VKC auf das Zielgerät zugreifen, kann es erforderlich sein, die maximale Aktualisierungsrate des Monitors zu ändern, damit die Aktualisierungsrate für das Zielgerät wirksam wird.

So stellen Sie die Aktualisierungsrate des Monitors ein:

1. Wählen Sie unter Windows® "Eigenschaften von Anzeige" > "Einstellungen" > "Erweitert" aus, um das Dialogfeld "Eigenschaften von Plug-and-Play-Monitor" zu öffnen.
2. Klicken Sie auf die Registerkarte "Monitor".
3. Setzen Sie die "Bildschirmaktualisierungsrate" auf einen höheren Wert als 100 Hz.
4. Klicken Sie auf "OK" und anschließend erneut auf "OK", um die Einstellungen zu übernehmen.

Mausoptionen

Bei der Steuerung eines Zielservers zeigt die Remotekonsole zwei Cursor an: Ein Cursor gehört zur Clientworkstation und der andere zum Zielserver.

Sie können entweder im Ein-Cursor-Modus oder im Zwei-Cursor-Modus arbeiten. Wenn Sie sich im Zwei-Cursor-Modus befinden und die Option ordnungsgemäß konfiguriert wurde, werden die Cursor aneinander ausgerichtet.

Bei zwei Cursorn bietet das Gerät verschiedene Mausmodi:

- Absolute (Mouse Synchronization) [Absolut (Maussynchronisierung)]
- Intelligent (Mouse Mode) [Intelligent (Mausmodus)]
- Standard (Mouse Mode) [Standard (Mausmodus)]



Mauszeigersynchronisierung

Bei der Remoteanzeige eines Zielservers mit einer Maus sehen Sie zwei Cursor: Ein Cursor gehört zur Remoteclientworkstation und der andere zum Zielserver. Wenn sich der Mauszeiger im Zielserverfenster des Virtual KVM Client befindet, werden Mausbewegungen und Klicks direkt an den angeschlossenen Zielserver übermittelt. Aufgrund der Mausbeschleunigungseinstellungen sind die Bewegungen des Clientmauszeigers etwas schneller als die des Zielgerätmauszeigers.

Bei schnellen LAN-Verbindungen sollten Sie den Mauszeiger des Virtual KVM Client deaktivieren, um nur den Cursor des Zielservers anzuzeigen. Sie können zwischen den beiden Modi (ein Cursor und zwei Cursor) wechseln.

Hinweis: Der VKC für den KX II-101 verwendet Symbole, die sich von den Symbolen, die im VKC für andere Dominion KX-Produkte unterscheiden. Weitere Informationen finden Sie unter VKC Toolbar for the KX II-101.

Tipps zur Maussynchronisierung

Führen Sie bei der Konfiguration der Maussynchronisierung folgende Schritte aus:

1. Stellen Sie sicher, dass die ausgewählte Videoauflösung und die Aktualisierungsfrequenz vom Gerät unterstützt werden. Im Dialogfeld "Virtual KVM Client Connection Info" (Virtual KVM Client – Verbindungsinformationen) werden die tatsächlich vom Gerät erkannten Werte angezeigt.
2. Stellen Sie sicher, dass die Kabellänge die Grenzwerte für die ausgewählte Videoauflösung nicht überschreitet.
3. Stellen Sie sicher, dass Maus und Monitor während der Installation richtig konfiguriert wurden.
4. Führen Sie eine automatische Erkennung durch, indem Sie im Virtual KVM Client auf die Schaltfläche "Auto-sense Video" (Video automatisch erkennen) klicken.
5. Führen Sie die folgenden Schritte aus, falls dadurch die Maussynchronisierung (bei Linux-, UNIX- und Solaris-KVM-Zielservern) nicht verbessert wird:
    a. Öffnen Sie ein Terminalfenster.
    b. Geben Sie den Befehl `xset mouse 1 1` ein.
    c. Schließen Sie das Terminalfenster.
6. Klicken Sie im Virtual KVM Client auf die Schaltfläche zur Maussynchronisierung .



Weitere Hinweise zum Mausmodus "Intelligent"

- Stellen Sie sicher, dass sich links oben auf dem Bildschirm keine Symbole oder Anwendungen befinden, da in diesem Bereich die Synchronisierungsroutine ausgeführt wird.
- Verwenden Sie keinen animierten Cursor.
- Deaktivieren Sie den Active Desktop auf KVM-Zielservern.

Synchronize Mouse (Maus synchronisieren)

Im Zwei-Cursor-Modus erzwingt der Befehl "Synchronize Mouse" (Maus synchronisieren) die erneute Ausrichtung des Zielserver-Mauszeigers am Mauszeiger des Virtual KVM Client.

Führen Sie einen der folgenden Schritte aus, um die Maus zu synchronisieren:

- Wählen Sie "Mouse" > "Synchronize Mouse" (Maus > Maus synchronisieren) aus oder klicken Sie auf die Schaltfläche "Synchronize Mouse" (Maus synchronisieren) in der Symbolleiste.

Mausmodus "Standard"

Beim Mausmodus "Standard" wird ein Standard-Maussynchronisierungsalgorithmus mit relativen Mauspositionen verwendet. Für den Mausmodus "Standard" müssen die Mausbeschleunigung deaktiviert und andere Mausparameter korrekt eingerichtet werden, damit die Client- und die Servermaus synchron bleiben. Der Mausmodus "Standard" ist voreingestellt.

So gelangen Sie in den Mausmodus "Standard":

- Wählen Sie "Mouse" > "Standard" (Maus > Standard) aus.



Mausmodus "Intelligent"

Im Mausmodus "Intelligent" erkennt das Gerät die Mauseinstellungen des Zielgeräts und kann die Cursor dementsprechend synchronisieren, wodurch die Mausbeschleunigung auf dem Zielgerät ermöglicht wird. In diesem Modus "tanzt" der Cursor in der oberen linken Ecke des Bildschirms und berechnet die Beschleunigung. Damit dieser Modus richtig funktioniert, müssen bestimmte Bedingungen erfüllt sein.

▶ So gelangen Sie in den Mausmodus "Intelligent":

- Wählen Sie "Mouse" > "Intelligent" (Maus > Intelligent) aus.

Bedingungen für die intelligente Maussynchronisierung

Der Befehl "Intelligent Mouse Synchronization" (Intelligente Maussynchronisierung) im Menü "Mouse" (Maus) synchronisiert automatisch die Cursor in Inaktivitätsphasen. Zur korrekten Synchronisierung müssen jedoch folgende Bedingungen erfüllt sein:

- Der Active Desktop muss auf dem Zielgerät deaktiviert sein.
- Oben in der linken Ecke auf der Zielseite dürfen keine Fenster angezeigt werden.
- Oben in der linken Ecke auf der Zielseite darf kein animierter Hintergrund vorhanden sein.
- Der Zielcursor muss standardmäßig und nicht animiert sein.
- Die Geschwindigkeit des Zielcursors darf nicht auf sehr hohe oder sehr niedrige Werte eingestellt sein.
- Erweiterte Mauseigenschaften wie "Enhanced pointer precision" (Zeigerbeschleunigung verbessern) oder "Snap mouse to default button in dialogs" (In Dialogfeldern automatisch zur Standardschaltfläche springen) müssen deaktiviert sein.
- Wählen Sie im Fenster "Video Settings" (Videoeinstellungen) die Option "Best Possible Video Mode" (Bestmöglicher Videomodus) aus.
- Die Ränder des Zielvideos müssen deutlich sichtbar sein. Ein schwarzer Rand muss also bei einem Bildlauf zu einem Rand des Zielvideobilds zwischen dem Zieldesktop und dem Fenster der KVM-Remotekonsole sichtbar sein.
- Wenn Sie die Funktion zur intelligenten Maussynchronisierung nutzen, können Datei- oder Ordnersymbole in der linken oberen Ecke Ihres Desktops zu Problemen führen. Um Probleme mit dieser Funktion zu vermeiden, empfiehlt Raritan, Datei- oder Ordnersymbole in der linken oberen Ecke Ihres Desktops zu entfernen.

Initiieren Sie nach dem automatischen Erkennen des Zielvideos manuell eine Maussynchronisierung. Klicken Sie dazu in der Symbolleiste auf die Schaltfläche "Synchronize Mouse" (Maus synchronisieren). Dies gilt auch bei Änderung der Auflösung des Zielgeräts, wenn die Cursor nicht mehr synchronisiert sind.

Schlägt die intelligente Maussynchronisierung fehl, wird die Standardeinstellung der Maussynchronisierung wiederhergestellt.

Beachten Sie, dass die Mauskonfigurationen auf unterschiedlichen Zielbetriebssystemen variieren. Weitere Informationen finden Sie in den Richtlinien für Ihr Betriebssystem. Die intelligente Maussynchronisierung ist für UNIX-Zielgeräte nicht verfügbar.

Mausmodus "Absolut"

In diesem Modus werden absolute Koordinaten verwendet, um die Cursor von Client und Zielgerät synchron zu halten, auch wenn für die Maus des Zielgeräts eine andere Beschleunigung oder Geschwindigkeit eingestellt wurde. Dieser Modus wird von Servern mit USB-Ports unterstützt.

So gelangen Sie in den Mausmodus "Absolut":

- Wählen Sie "Mouse" > "Absolute" (Maus > Absolut) aus.

Hinweis: Die absolute Mauseinstellung erfordert ein USB-Zielsystem und wird als Mauseinstellung für den KX II-101 empfohlen.

Hinweis: Der Mausmodus "Absolute Mouse Synchronization" (Absolute Maussynchronisierung) steht nur für USB-CIMs (D2CIM-VUSB und D2CIM-DVUSB) mit Aktivierung für virtuelle Medien zur Verfügung.

Ein Cursor

Beim Ein-Cursor-Modus wird nur der Cursor des Zielservers verwendet; der lokale Mauszeiger wird nicht mehr angezeigt. Im Ein-Cursor-Modus steht der Befehl "Synchronize Mouse" (Maus synchronisieren) nicht zur Verfügung, da ein einzelner Mauszeiger nicht synchronisiert werden muss.

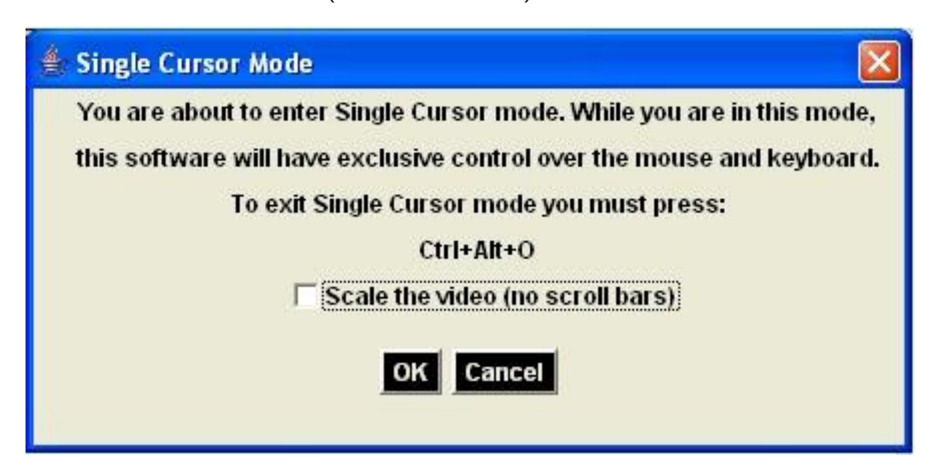
Hinweis: Der VKC für den KX II-101 verwendet Symbole, die sich von den Symbolen, die im VKC für andere Dominion KX-Produkte unterscheiden. Weitere Informationen finden Sie unter VKC Toolbar for the KX II-101.

Führen Sie folgende Schritte aus, um den Ein-Cursor-Modus zu aktivieren:

1. Wählen Sie "Mouse" > "Single Mouse Cursor" (Maus > Ein Cursor) aus.



2. Klicken Sie in der Symbolleiste auf die Schaltfläche "Single/Double Mouse Cursor" (Ein/Zwei Cursor).



So beenden Sie den Ein-Cursor-Modus:

1. Drücken Sie "Strg+Alt+O" auf der Tastatur, um den Ein-Cursor-Modus zu beenden.

VKC Virtual Media (Virtuelle Medien)

Umfassende Informationen zum Einrichten und Verwenden virtueller Medien finden Sie im Kapitel Virtuelle Medien.

Smart Cards (VKC, AKC und MPC)

Wenn Sie den KX II 2.1.10 oder höher verwenden, können Sie ein Smart Card-Lesegerät auf dem Zielserver mounten, um die Smart Card-Authentifizierung und die damit verbundenen Anwendungen zu unterstützen. Eine Liste der unterstützten Smart Cards und Smart Card-Lesegeräte und Informationen zu zusätzlichen Systemanforderungen finden Sie unter ***Unterstützte und nicht unterstützte Smart Card-Lesegeräte*** (auf Seite 326).

Beim Remote-Zugriff auf den Server haben Sie die Möglichkeit, ein angeschlossenes Smart Card-Lesegerät auszuwählen und auf dem Server zu mounten. Der Zielserver verwendet Smart Card-Authentifizierung. Diese Art der Authentifizierung wird nicht beim Anmelden am Gerät verwendet. Änderungen bezüglich der Smart Card-PIN und den Anmeldeinformationen erfordern daher keine Aktualisierungen der Gerätekonten. Nach der Installation des Kartenlesegeräts und der Smart Card auf dem Zielserver, funktioniert der Server so, als wären das Kartenlesegerät und die Smart Card direkt am Server angeschlossen. Abhängig von den Einstellungen in den Richtlinien zur Entfernung der Karte im Betriebssystem des Zielservers wird beim Entfernen der Smart Card oder des Smart Card-Lesegeräts die Benutzersitzung gesperrt, oder Sie werden abgemeldet. Ist die KVM-Sitzung unterbrochen, weil Sie beendet wurde oder Sie auf ein neues Ziel umgeschaltet haben, wird das Smart Card-Kartenlesegerät automatisch vom Zielserver deinstalliert.

Wenn auf dem Gerät der Modus "PC-Share" (PC-Freigabe) aktiviert ist, können mehrere Benutzer gleichzeitig auf den Zielserver zugreifen. Ist jedoch ein Smart Card-Lesegerät an das Ziel angeschlossen, ist, unabhängig vom Modus "PC-Share" (PC-Freigabe), nur der exklusive Zugriff möglich. Zusätzlich ist das Smart Card-Lesegerät während einer gemeinsamen Sitzung deaktiviert, bis der exklusive Zugriff auf den Server verfügbar wird.

Nach dem Herstellen einer KVM-Verbindung zum Zielserver, werden ein Smart Card-Menü und eine Smart Card-Schaltfläche im Virtual KVM Client und im Multi-Platform-Client verfügbar. Nachdem das Menü geöffnet oder auf die Smart Card-Schaltfläche geklickt wurde, werden die Smart Card-Lesegeräte angezeigt, die als an den Remoteclient angeschlossen erkannt werden. In diesem Dialogfeld können Sie weitere Smart Card-Lesegeräte hinzufügen, die Liste der an das Ziel angeschlossenen Smart Card-Lesegeräte aktualisieren und Smart Card-Lesegeräte entfernen. Sie können auch eine Smart Card entfernen oder wieder einführen. Diese Funktion kann verwendet werden, um das Betriebssystem eines Zielservers zu benachrichtigen, das das Entfernen und Wiedereinführen erfordert, um das entsprechende Dialogfeld für die Anmeldung anzuzeigen. Mithilfe dieser Funktion kann die Benachrichtigung an ein individuelles Ziel gesendet werden, ohne andere KVM-Sitzungen zu beeinträchtigen.



So mounten Sie ein Smart Card-Lesegerät:

1. Klicken Sie auf das Menü "Smart Card", und wählen Sie anschließend "Smart Card Reader" (Smart Card-Lesegerät) aus. Sie können auch in der Symbolleiste auf die Schaltfläche "Smart Card" klicken.
2. Wählen Sie im Dialogfeld "Select Smart Card Reader" (Smart Card-Lesegerät auswählen) das Smart Card-Lesegerät aus.
3. Klicken Sie auf "Mount".
4. Ein Dialogfeld wird geöffnet, in dem der Fortschritt angezeigt wird. Aktivieren Sie das Kontrollkästchen "Mount selected card reader automatically on connection to targets" (Ausgewähltes Kartenlesegerät bei Verbindung zu Zielen automatisch mounten), um das Smart Card-Lesegerät automatisch zu installieren, wenn Sie das nächste Mal eine Verbindung zu einem Ziel herstellen. Klicken Sie auf "OK", um den Installationsvorgang zu starten.

So aktualisieren Sie die Smart Card im Dialogfeld "Select Smart Card Reader" (Smart Card-Lesegerät auswählen):

- Klicken Sie auf "Refresh List" (Liste aktualisieren), wenn Sie ein neues Smart Card-Lesegerät an den Cient-PC angeschlossen haben.

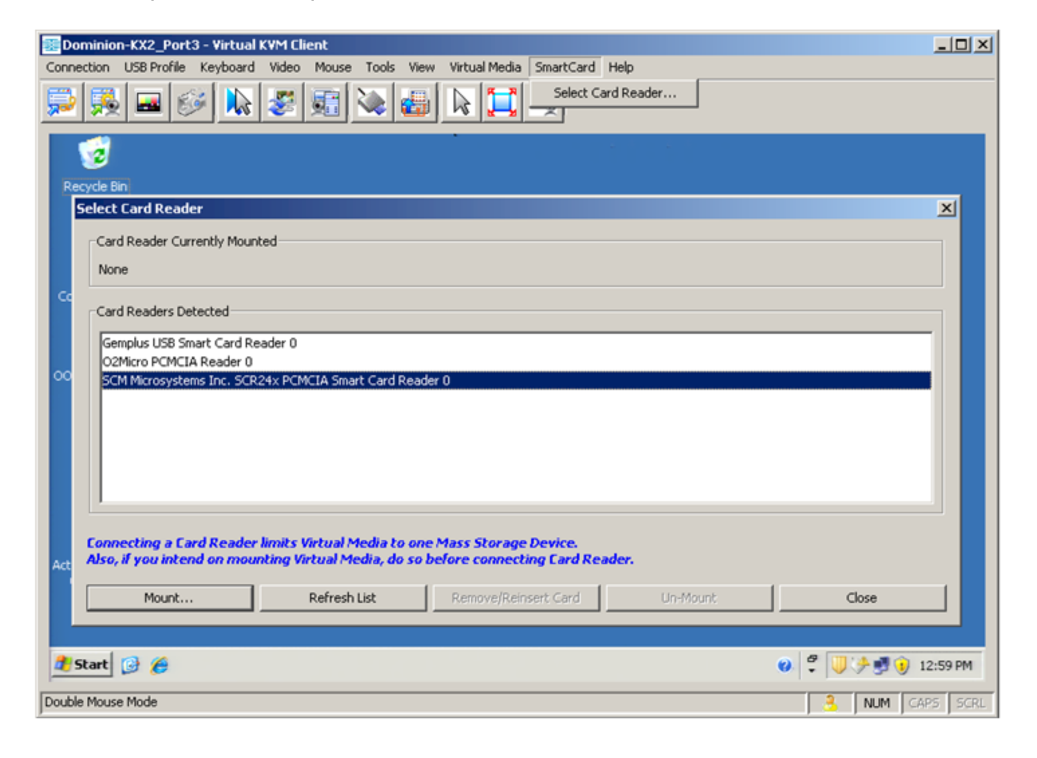
So senden Sie Benachrichtigungen über das Entfernen und Wiedereinführen einer Smart Card an das Ziel:

- Wählen Sie das aktuell installierte Smart Card-Lesegerät aus, und klicken Sie auf die Schaltfläche "Remove/Reinsert" (Entfernen/Wiedereinführen).

So unmounten Sie ein Smart Card-Lesegerät:

- Wählen Sie das Smart Card-Lesegerät aus, das Sie unmouten möchten, und klicken Sie auf die Schaltfläche "Unmount".

Das Mounten von Smart Card-Lesegeräten wird auch von der lokalen Konsole unterstützt. Siehe **Smart Card-Zugriff von der lokalen Konsole** (auf Seite 287) in der KX II-Hilfe.





Optionen im Menü "Tools" (Extras)

Im Menü "Tools" (Extras) können Sie bestimmte Optionen für die Verwendung mit dem Virtual KVM Client einstellen (einschließlich Protokollierung, Einstellen des Tastaturtyps und Definieren von Zugriffstasten zum Beenden des Vollbild- und Ein-Cursor-Modus).

So legen Sie die Optionen im Menü "Tools" (Extras) fest:

1. Wählen Sie "Tools" > "Options" (Extras > Optionen) aus. Das Dialogfeld "Options" (Optionen) wird angezeigt.
2. Aktivieren Sie das Kontrollkästchen "Enable Logging" (Protokollierung aktivieren) nur nach Anweisung durch den technischen Kundendienst. Bei dieser Option wird im Basisverzeichnis eine Protokolldatei erstellt.
3. Wählen Sie ggf. in der Dropdownliste "Keyboard Type" (Tastaturtyp) einen Tastaturtyp aus. Folgende Optionen stehen zur Verfügung:
   - US/International (USA/International)
   - French (France) (Französisch)
   - German (Germany) (Deutsch, Deutschland)
   - Japanisch
   - United Kingdom (Großbritannien)
   - Korean (Korea) (Koreanisch)
   - Belgian (Belgium) (Belgisch)
   - Norwegian (Norway) (Norwegisch)
   - Portugiesisch (Portugal)
   - Danish (Denmark) (Dänisch)
   - Swedish (Sweden) (Schwedisch)
   - German (Deutsch, Schweiz)
   - Hungarian (Hungary) (Ungarisch)
   - Spanish (Spain) Spanisch
   - Italian (Italy) (Italienisch)
   - Slowenisch
   - Übersetzung: Französisch – Englisch (USA)
   - Übersetzung: Französisch – Englisch (USA/International)

   Hinweis: Beim AKC entspricht der Tastaturtyp standardmäßig dem lokalen Client. In diesem Fall trifft die Option nicht zu.

4. Exit Full Screen Mode - Hotkey (Zugriffstaste zum Beenden des Vollbildmodus). Wenn Sie in den Vollbildmodus wechseln, erscheint die Anzeige des Zielservers im Vollbildmodus mit derselben Auflösung wie auf dem Zielserver. Diese Zugriffstaste wird zum Beenden des Modus verwendet.
5. Exit Single Cursor Mode - Hotkey. (Zugriffstaste zum Beenden des Ein-Cursor-Modus). Im Ein-Cursor-Modus wird nur der Cursor des Zielservers angezeigt. Diese Zugriffstaste wird zum Beenden des Ein-Cursor-Modus verwendet, sodass der Client-Cursor wieder angezeigt wird. Klicken Sie auf OK.

Client Launch Settings (Client-Starteinstellungen)

KX II-Benutzer können auch die Starteinstellungen für den Client konfigurieren, um die Größe des Bildschirms für eine KVM-Sitzung zu definieren.

6. Wählen Sie die Registerkarte "Client Launch Settings" (Client-Starteinstellungen) aus.
   a. So konfigurieren Sie die Zielfenstereinstellungen:
   - Wählen Sie "Standard - sized to target Resolution" (Standard - Größe an Zielauflösung anpassen) aus, um das Fenster mit der aktuellen Auflösung des Ziels zu öffnen. Wenn die Zielauflösung größer als die Client-Auflösung ist, bedeckt das Zielfenster soviel Bildschirmfläche wie möglich. Gegebenenfalls werden Bildlaufleisten hinzugefügt.
   - Wählen Sie "Full Screen" (Vollbild) aus, um das Fenster im Vollbildmodus zu öffnen.

   a. So konfigurieren Sie den Monitor, auf dem der Ziel-Viewer gestartet wird:
   - Wählen Sie "Monitor Client Was Launched from" (Monitor-Client gestartet von) aus, wenn der Ziel-Viewer in derselben Anzeige wie die auf dem Client verwendete Anwendung gestartet werden soll (z. B. ein Webbrowser oder ein Applet).
7. Wählen Sie "Select From Detected Monitors" (Aus gefundenen Monitoren auswählen) aus, um einen Monitor aus einer Liste mit Zielmonitoren auszuwählen, die von der Anwendung gefunden wurden. Wenn ein zuvor ausgewählter Monitor nicht mehr gefunden wird, wird "Currently Selected Monitor Not Detected" (Aktuell ausgewählter Monitor nicht gefunden) angezeigt.
8. Klicken Sie auf OK.



Tastaturbeschränkungen

Slowenische Tastaturen

Aufgrund einer JRE-Beschränkung funktioniert die Taste < auf slowenischen Tastaturen nicht.

Sprachkonfiguration für Linux

Da mit der Sun-JRE auf einem Linux-Betriebssystem Probleme bei der korrekten Erzeugung von KeyEvents (Tastenereignissen) für fremdsprachige Tastaturen auftreten, die mithilfe der Systemeinstellungen konfiguriert wurden, empfiehlt Raritan die Konfiguration fremdsprachiger Tastaturen mithilfe der in der folgenden Tabelle beschriebenen Methoden.

Sprache	Konfigurationsmethode
USA/Int.	Standard
Französisch	Keyboard Indicator (Tastaturanzeige)
Deutsch (Deutschland)	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Japanisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Britisches Englisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Koreanisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Belgisch	Keyboard Indicator (Tastaturanzeige)
Norwegisch	Keyboard Indicator (Tastaturanzeige)
Dänisch	Keyboard Indicator (Tastaturanzeige)
Schwedisch	Keyboard Indicator (Tastaturanzeige)
Ungarisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Spanisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Italienisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Slowenisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Portugiesisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]

Hinweis: Die Tastaturanzeige sollte bei Linux-Systemen, die Gnome als Desktopumgebung nutzen, verwendet werden.



Ansichtsoptionen

"View Toolbar" (Symbolleiste anzeigen)

Sie können den Virtual KVM Client mit oder ohne die Symbolleiste verwenden.

So blenden Sie die Symbolleiste ein bzw. aus:

- Wählen Sie **View > View Toolbar** (Ansicht > Symbolleiste anzeigen).

"Scaling" Skalieren

Das Skalieren des Zielfensters ermöglicht die Anzeige des gesamten Inhalts des Zielserverfensters. Dieses Feature vergrößert oder verkleinert das Zielvideobild unter Beibehaltung des Seitenverhältnisses, um es an die Fenstergröße des Virtual KVM Client anzupassen. Somit wird der gesamte Zielserverdesktop angezeigt, und Sie müssen nicht die Bildlaufleiste verwenden.

So aktivieren bzw. deaktivieren Sie die Skalierung:

- Wählen Sie **View > Scaling** (Ansicht > Skalieren).

Target Screen Resolution (Zielbildschirmauflösung)

Wenn Sie in den Vollbildmodus wechseln, erscheint die Anzeige des Zielservers im Vollbildmodus mit derselben Auflösung wie auf dem Zielserver. Die Zugriffstaste, über die Sie diesen Modus beenden können, legen Sie im Dialogfeld "Options" (Optionen) fest. Standardmäßig lautet die Tastenkombination "Strg+Alt+M". Wenn Sie im Vollbildmodus den Mauszeiger an den oberen Bildschirmrand schieben, wird die Menüleiste für den Vollbildschirmmodus angezeigt.

So gelangen Sie in den Vollbildmodus:

- Wählen Sie "View" > "Full Screen" (Ansicht > Vollbild) aus.

So beenden Sie den Vollbildmodus:

- Drücken Sie die im Extras-Dialogfeld "Options" (Optionen) konfigurierte Zugriffstaste. Standardmäßig lautet die Tastenkombination "Strg+Alt+M". Wählen Sie für AKC "Connection/Exit" (Verbindung/Beenden) aus der ausgeblendeten Menüleiste, indem Sie zuvor den Mauszeiger an den oberen Bildschirmrand bewegen.

Wenn Sie immer im Vollbildmodus auf das Ziel zugreifen möchten, können Sie den Vollbildmodus als Standardeinstellung auswählen.

So aktivieren Sie den Vollbildmodus als Standardmodus:

1. Klicken Sie auf "Tools" (Extras) > "Options" (Optionen), um das Dialogfeld "Options" (Optionen) zu öffnen.

2. Wählen Sie "Enable Launch in Full Screen Mode" (Start im Vollbildmodus aktivieren), und klicken Sie auf "OK".

Hilfeoptionen

About Raritan Virtual KVM Client (Informationen zum Raritan Virtual KVM Client)

Dieser Menübefehl liefert Versionsinformationen zum Virtual KVM Client, falls Sie Unterstützung durch den technischen Kundendienst von Raritan benötigen.

So rufen Sie die Versionsinformationen ab:

1. Wählen Sie "Help" > "About Raritan Virtual KVM Client" (Hilfe > Informationen zum Raritan Virtual KVM Client) aus.
2. Verwenden Sie die Schaltfläche "Copy to Clipboard" (In Zwischenablage kopieren), um die im Dialogfeld enthaltenen Informationen in eine Zwischenablagedatei zu kopieren, sodass auf diese bei Bedarf später bei Hilfestellung durch den Kundendienst zugegriffen werden kann.



Active KVM Client (AKC)

Überblick

Der Microsoft Windows .NET-basierte Active KVM Client (AKC) ist mit dem KX II 2.2 (oder höher) erhältlich und unterstützt alle KX II-Modelle mit Ausnahme der Modelle KX2-101 und KSX2, die derzeit noch nicht unterstützt werden. Der AKC basiert auf Microsoft Windows .NET-Technologie. Benutzer können den Client in Windows-Umgebungen ausführen, ohne die Java Runtime Environment (JRE) zu verwenden, welche zur Ausführung der Clients Virtual KVM und Multi-Platform von Raritan erforderlich ist. Der AKC funktioniert auch mit CC-SG.

Der AKC und VKC verfügen mit Ausnahme der nachfolgend aufgeführten Punkte über identische Leistungsmerkmale:

- Mindestanforderungen an das System
- Unterstützte Betriebssysteme und Browser
- Auf dem AKC erstellte Tastaturmakros können im VKC nicht genutzt werden.

Weitere Informationen zu den verfügbaren Funktionen der Anwendung finden Sie im Abschnitt ***Virtual KVM Client*** (auf Seite 63). In diesem Abschnitt werden auch Unterschiede zwischen den Funktionen des AKC und des VKC aufgeführt.

Informationen zur Konfiguration bei der Verwendung von AKC finden Sie unter ***Aktivieren des direkten Portzugriffs*** (siehe "***Aktivieren des direkten Port-Zugriffs***" auf Seite 171) und ***Aktivieren der AKC-Download-Serverzertifikat-Validierung*** (auf Seite 172).

Hinweis: Wenn Sie direkten Portzugriff mit dem AKC nutzen, müssen Sie für jedes Ziel, auf das Sie zugreifen möchten, ein neues Browser-Fenster oder eine neue Browser-Registerkarte öffnen. Wenn Sie versuchen, auf ein weiteres Ziel zuzugreifen, indem Sie die DPA-URL im selben Browser-Fenster oder derselben Browser-Registerkarte eingeben, von der aus Sie gerade auf ein Ziel zugreifen, wird keine Verbindung hergestellt, und Sie erhalten eine Fehlermeldung.

Vom AKC unterstützte Betriebssysteme und Browser

.NET Framework

Der AKC benötigt .NET® Version 3.5 und funktioniert sowohl mit Version 3.5 als mit Version 4.0.

Betriebssysteme

Wurde der AKC über Internet Explorer® oder als eigenständige Anwendung gestartet, bietet er Ihnen die Möglichkeit, über KX II 2.2 (oder höher) auf Zielserver zuzugreifen. Der AKC ist mit den folgenden Plattformen kompatibel, auf denen .NET Framework 3.5 ausgeführt wird:

- Windows XP®-Betriebssystem
- Windows Vista®-Betriebssystem (bis 64 Bit)
- Windows Vista®-Betriebssystem (bis 64 Bit)

Hinweis: Sie müssen Windows 7 verwenden, wenn WINDOWS PC FIPs aktiviert ist und Sie mithilfe von AKC und einer Smart Card auf ein Ziel zugreifen.

Da .NET für die Ausführung von AKC benötigt wird, erhalten Sie, wenn Sie .NET nicht oder eine nicht unterstützte Version von .NET installiert haben, eine Meldung, in der Sie aufgefordert werden, die Version von .NET zu prüfen.

Browser

- Internet Explorer 6 oder höher

Wenn Sie versuchen, den AKC über einem anderen Browser als IE 6 oder höher zu öffnen, wird Ihnen eine Fehlermeldung angezeigt, in der Sie aufgefordert werden, zu prüfen, welchen Browser Sie verwenden und ggf. Internet Explorer zu verwenden.



Voraussetzungen für die Verwendung des AKC

So verwenden Sie den AKC:

- Stellen Sie sicher, dass die Cookies von der IP-Adresse des Geräts, auf das zugegriffen wird, nicht blockiert werden.
- Die Benutzer von Windows Vista-, Windows 7- und Windows 2008-Servern müssen sicherstellen, dass die IP-Adresse des Geräts, auf das zugegriffen wird, in der Zone "Vertrauenswürdige Sites" hinzugefügt wurde und dass der "Geschützte Modus" nicht aktiv ist, wenn auf das Gerät zugegriffen wird.

Enable AKC Download Server Certificate Validation (AKC-Download-Serverzertifikat-Validierung aktivieren)

Falls durch den KX II-Administrator (oder CC-SG-Administrator) die Option "Enable AKC Download Server Certificate Validation" (AKC-Download-Serverzertifikat-Validierung aktivieren) aktiviert wurde:

- Administratoren müssen ein gültiges Zertifikat zu KX II hochladen oder ein selbstsigniertes Zertifikat auf KX II generieren. Das Zertifikat muss über eine gültige Hostbezeichnung verfügen.
- Jeder Benutzer muss das CA-Zertifikat (oder eine Kopie des selbstsignierten Zertifikats) zum Speicher für "Vertrauenswürdige Stammzertifizierungsstellen" seines Browsers hinzufügen.

Zum Starten von AKC über den CC-SG-Admin-Client müssen Sie über JRE™ 1.6.0_10 oder höher verfügen.



Kapitel 4 Powerstrip-Ausgangssteuerung (Gestell-PDU)

In diesem Kapitel

Überblick

Mit Dominion KX II können Sie Powerstrip-Ausgänge der Serien Raritan PX und Raritan RPC steuern, die über ein D2CIM-PWR mit Dominion KX II verbunden sind.

Ist ein PX oder ein RPC eingerichtet und an Dominion KX II angeschlossen, können der Powerstrip und die Ausgänge über die Seite "Powerstrip" der Dominion KX II-Benutzeroberfläche gesteuert werden. Sie können auf diese Seite zugreifen, indem Sie auf das Menü "Power" (Strom) oben auf der Seite klicken.

Die Seite "Powerstrip" zeigt an Dominion KX II angeschlossene Powerstrips an, für die der Benutzer entsprechende Portzugriffsberechtigungen erhalten hat. Bei Schichtkonfigurationen zeigt die Seite "Powerstrip" Powerstrips an, die an Dominion KX II-Basis- und Schichtgeräte angeschlossen sind, für die der Benutzer entsprechende Portzugriffsberechtigungen erhalten hat.

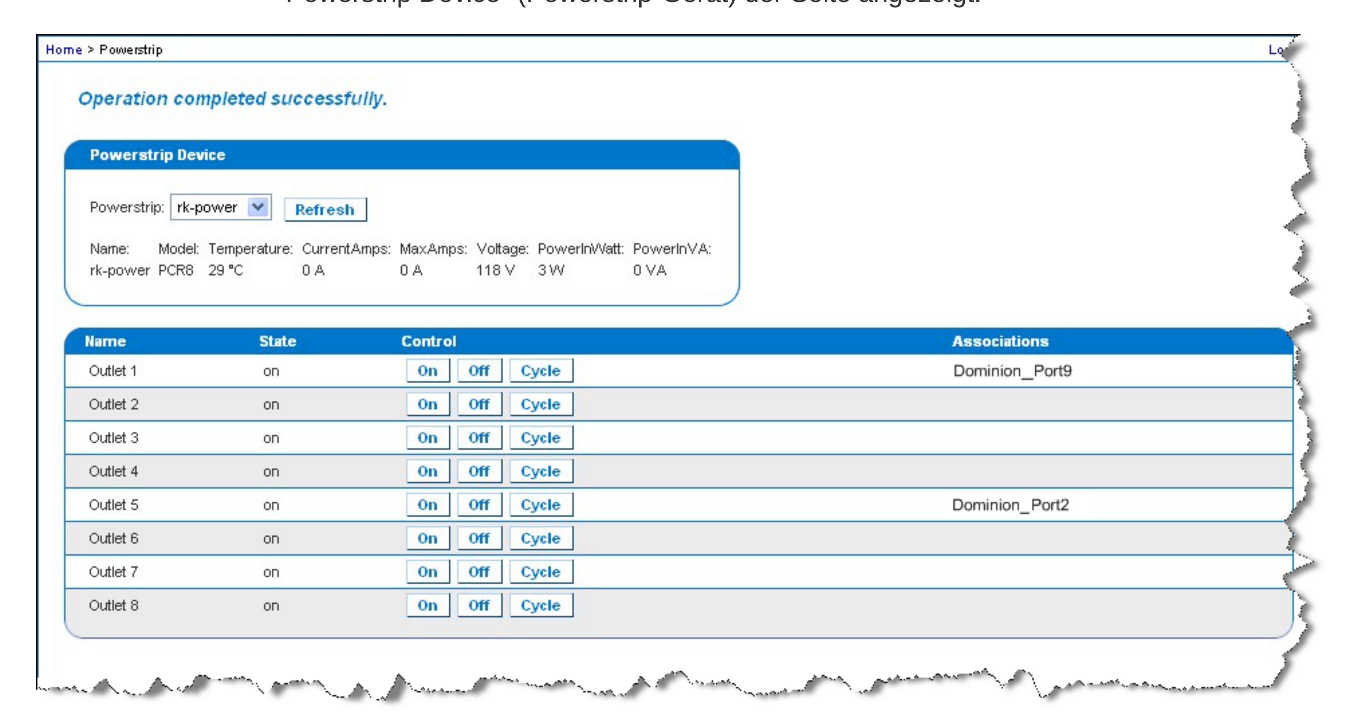
Hinweis: Informationen zum Einrichten eines PX finden Sie im ***Benutzerhandbuch für Dominion PX****.*

Auf der Seite "Powerstrip" können Sie die Ausgänge einschalten und ausschalten sowie aus- und wieder einschalten. Sie können außerdem die folgenden Informationen zu Powerstrip und Ausgang anzeigen:

- Powerstrip-Geräteinformationen:
  - Name
  - Model (Modell)
  - Temperatur
  - Current Amps (Aktuelle Stromstärke)
  - Maximum Amps (Maximale Stromstärke)
  - Voltage (Spannung)
  - Power in Watts (Strom in Watt)
  - Power in Volts Ampere (Strom in Voltampere)

- Ausgangsanzeigeinformationen:
  - Name – Der Name, der dem Ausgang bei der Konfiguration zugeordnet wurde.
  - State (Status) – Status des Ausgangs (Ein/Aus)
  - Control (Steuerung) – Ausgänge einschalten und ausschalten sowie aus- und wieder einschalten
  - Association (Zuordnung) – Die dem Ausgang zugeordneten Ports

Wenn Sie die Seite "Powerstrip" öffnen, werden die Powerstrips, die zurzeit mit Dominion KX II verbunden sind, zunächst in der Dropdown-Liste "Powerstrip" angezeigt. Außerdem werden Informationen zum aktuell ausgewählten Powerstrip angezeigt. Wenn keine Powerstrips mit Dominion KX II verbunden sind, wird die Meldung "No powerstrips found" (Keine Powerstrips gefunden) im Abschnitt "Powerstrip Device" (Powerstrip-Gerät) der Seite angezeigt.



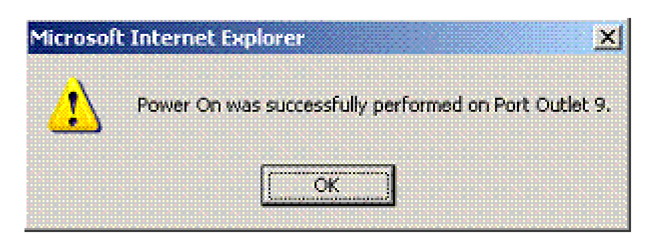
Einschalten und Ausschalten sowie Ein- und Ausschalten von Ausgängen

▶ So schalten Sie einen Ausgang ein:

1. Klicken Sie auf das Menü "Power" (Strom), um die Seite "Powerstrip" zu öffnen.
2. Wählen Sie aus der Dropdown-Liste "Powerstrip" den PX-Powerstrip aus, den Sie einschalten möchten.



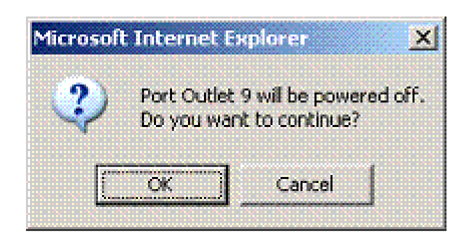
3. Klicken Sie auf "Refresh" (Aktualisieren), um die Stromzufuhrsteuerung anzuzeigen.
4. Klicken Sie auf "On" (Ein).



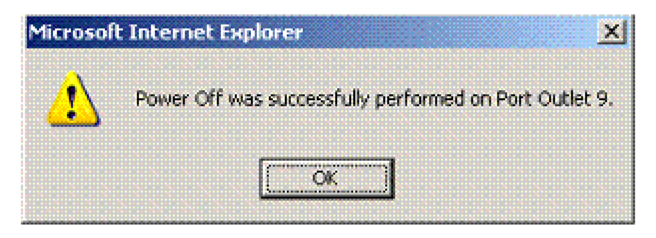
5. Klicken Sie auf OK, um das Bestätigungsdialogfeld "Power On" (Strom ein) zu schließen. Der Ausgang schaltet sich ein und der Status wird als "On" (Ein) angezeigt.

So schalten Sie einen Ausgang aus:

1. Klicken Sie auf "Off" (Aus).
2. Klicken Sie im Dialogfeld "Power Off" (Strom aus) auf OK.



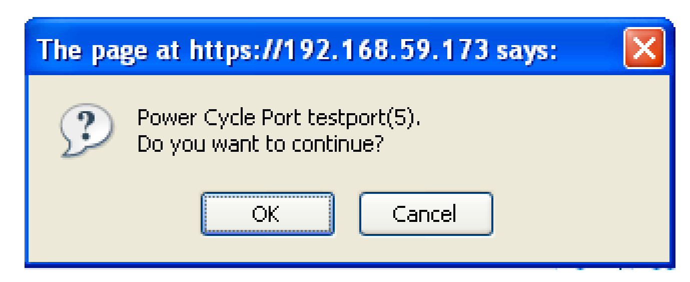
3. Klicken Sie im Bestätigungsdialogfeld "Power Off" (Strom aus) auf OK. Der Ausgang schaltet sich aus und der Status wird als "Off" (Aus) angezeigt.



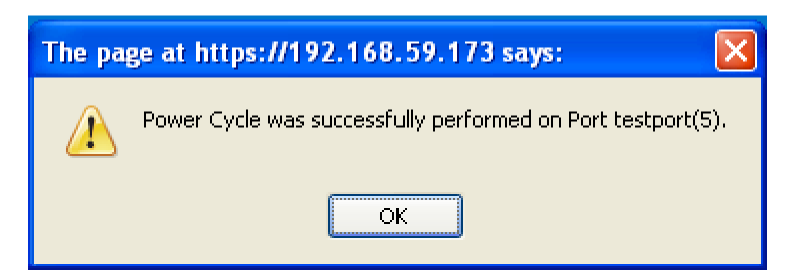


So schalten Sie einen Ausgang aus und wieder ein:

1. Klicken Sie auf die Schaltfläche "Cycle" (Aus- und Einschalten). Das Dialogfeld "Power Cycle Port" (Port aus- und wieder einschalten) wird geöffnet.



2. Klicken Sie auf OK. Der Ausgang wird nun aus- und wieder eingeschaltet (dies kann einige Sekunden dauern).



3. Wenn der Vorgang abgeschlossen ist, öffnet sich ein Dialogfenster. Klicken Sie zum Schließen des Dialogfensters auf OK.

Kapitel 5 Virtual Media (Virtuelle Medien)

In diesem Kapitel



Überblick

Virtuelle Medien erweitern die KVM-Funktionen. Sie ermöglichen KVM-Zielservern den Remotezugriff auf Medien auf einem Client-PC und Netzwerkdateiservern. Dank dieses Features werden auf dem Client-PC und Netzwerkdateiservern installierte Medien praktisch virtuell vom Zielserver installiert. Der Zielserver hat Lese- und Schreibzugriff auf die Medien, als wären sie physisch mit dem Zielserver verbunden. Zusätzlich zur Unterstützung von Datendateien über virtuelle Medien werden Dateien von virtuellen Medien über USB-Verbindung unterstützt.

Virtuelle Medien können interne und per USB angeschlossene CD- und DVD-Laufwerke, USB-Massenspeichergeräte, PC-Festplatten und ISO-Abbilder (Datenträgerabbilder) umfassen.

Hinweis: ISO9660 wird standardmäßig von Raritan unterstützt. Andere ISO-Standards können jedoch ebenfalls verwendet werden.

Virtuelle Medien bieten die Möglichkeit, weitere Aufgaben von einem Remotestandort aus zu erledigen. Dazu zählen:

- Übertragen von Dateien
- Durchführen von Diagnosen
- Installieren oder Reparieren von Anwendungen
- Vollständiges Installieren des Betriebssystems

Diese erweiterte KVM-Steuerung macht die meisten Gänge in das Rechenzentrum überflüssig, spart Zeit und Geld und unterstreicht damit die Bedeutung virtueller Medien.


Raritan.

Diagrammschlüssel			
1	Desktop-PC	A	CD-/DVD-Laufwerk
2	Dominion KX II	B	USB-Massenspeichergerät
3	CIM	C	PC-Festplatte
4	Zielserver	D	Remote-Dateiserver (ISO-Abbilder)

Voraussetzungen für die Verwendung virtueller Medien

Mit dem Feature für virtuelle Medien können Sie bis zu zwei Laufwerke (verschiedenen Typs) mounten, die durch das aktuell dem Zielgerät zugeordnete USB-Profil unterstützt werden. Diese Laufwerke sind während der KVM-Sitzung zugänglich.

Sie können beispielsweise eine bestimmte CD-ROM installieren, verwenden und nach Fertigstellung Ihrer Arbeit wieder trennen. Der virtuelle Medienkanal für CD-ROMs bleibt jedoch offen, sodass Sie eine andere CD-ROM virtuell installieren können. Diese virtuellen Medienkanäle bleiben offen, bis die KVM-Sitzung geschlossen wird (vorausgesetzt, sie werden vom USB-Profil unterstützt).

Um das virtuelle Medium zu verwenden, schließen Sie es an den Client-PC oder Netzwerkdateiserver an, auf den Sie über den Zielserver zugreifen möchten. Dieser Schritt muss nicht als erster erfolgen, jedoch bevor Sie versuchen, auf das Medium zuzugreifen.

Für die Verwendung virtueller Medien müssen folgende Bedingungen erfüllt sein:

Dominion-Gerät

- Für Benutzer, die Zugriff auf virtuelle Medien benötigen, müssen die Geräteberechtigungen für den Zugriff auf die relevanten Ports sowie der virtuelle Medienzugriff (Portberechtigung VM Access [VM-Zugriff]) für diese Ports eingerichtet werden. Portberechtigungen werden auf Gruppenebene eingerichtet.
- Zwischen dem Gerät und dem Zielserver muss eine USB-Verbindung bestehen.
- Wenn Sie die PC-Freigabe verwenden möchten, müssen die Security Settings (Sicherheitseinstellungen) auf der Seite "Security Settings" (Sicherheitseinstellungen) aktiviert sein. **Optional**
- Sie müssen das richtige USB-Profil für den KVM-Zielserver auswählen, zu dem Sie eine Verbindung herstellen.

Client-PC

- Für bestimmte virtuelle Medienoptionen sind Administratorrechte auf dem Client-PC erforderlich (z. B. Umleitung ganzer Laufwerke).

Hinweis: Wenn Sie Windows Vista or Windows 7 verwenden, deaktivieren Sie "User Account Control" (Benutzerkontensteuerung), oder wählen Sie beim Start von Internet Explorer "Run as Administrator" (Als Administrator ausführen) aus. Klicken Sie dazu auf das Menü "Start", klicken Sie mit der rechten Maustaste auf "Internet Explorer", und wählen Sie "Run as Administrator" (Als Administrator ausführen) aus.



Zielserver

- KVM-Zielserver müssen über USB angeschlossene Laufwerke unterstützen.
- Auf KVM-Zielservern mit Windows 2000 müssen alle aktuellen Patches installiert sein.
- USB 2.0-Ports sind schneller und daher vorzuziehen.

Verwenden von virtuellen Medien über den VKC und den AKC in einer Windows-Umgebung

Die Berechtigungen für den Systemadministrator und Standardbenutzer unter dem Betriebssystem Windows XP® unterscheiden sich von den Berechtigungen unter den Betriebssystemen Windows Vista® und Windows 7®.

Ist die "User Access Controll (UAC)" (Benutzerzugriffssteuerung) unter Windows Vista oder Windows 7 aktiviert, so bietet diese die Berechtigungen der niedrigsten Stufe, die ein Benutzer für eine Anwendung benötigt. Beispielsweise ist die Option "Run as Administrator" (Als Administrator ausführen) für Internet Explorer® verfügbar, um Benutzern die Ausführung spezieller Aufgaben auf Administratorebene zu gestatten. Diese Berechtigung würde sonst nicht bestehen, selbst wenn der Benutzer über ein Administratorkonto verfügt.

Diese beiden Funktionen wirken sich darauf aus, auf welchen Typ virtueller Medien von Benutzern über den Virtual KVM Client (VKC) und den Active KVM Client (AKC) zugegriffen werden kann. Weitere Informationen zu diesen Funktionen und deren Verwendung finden Sie in Ihrer Microsoft®-Hilfe.

Im Folgenden finden Sie eine Liste mit Typen virtueller Medien, auf die über den VKC und den AKC aus einer Windows-Umgebung zugegriffen werden kann. Die Funktionen sind nach Client-Funktionen und Funktionen der virtuellen Medien aufgeteilt, die den einzelnen Windows-Benutzerfunktionen zugewiesen sind.

Windows XP

- Wenn Sie den VKC und den AKC in einer Windows XP-Umgebung ausführen, müssen Benutzer über Administratorrechte verfügen, um auf andere Medientypen als CD-ROM-Verbindungen, ISO-Dateien und ISO-Abbilder zugreifen zu können.

Windows Vista und Windows 7

- Wenn Sie den VKC und den AKC in einer Windows Vista- oder Windows 7-Umgebung bei aktivierter UAC ausführen, kann, je nach Windows-Benutzerfunktion, auf die folgenden virtuellen Medientypen zugegriffen werden.

Client	Administrator	Standard-Benutzer
AKC und VKC	Zugriff auf: • Fest installierte Laufwerke und deren Partitionen • Wechsellaufwerke • CD-/DVD-Laufwerke • ISO-Abbilder • Remote-ISO-Abbilder	Zugriff auf: • Wechsellaufwerke • CD-/DVD-Laufwerke • ISO-Abbilder • Remote-ISO-Abbilder

Verwenden virtueller Medien

Lesen Sie die Hinweise zu den Voraussetzungen für die Verwendung virtueller Medien, bevor Sie mit der Verwendung virtueller Medien fortfahren.

So verwenden Sie virtuelle Medien:

1. Wenn Sie auf Dateiserver-ISO-Abbilder zugreifen möchten, lassen Sie diese Dateiserver und Abbilder über die Seite "Remote Console File Server Setup" (Remotekonsolen-Dateiserver-Setup) erkennen. Siehe Dateiserver-Setup (nur für Dateiserver-ISO-Abbilder).

   Hinweis: Das ISO9660-Format wird standardmäßig von Raritan unterstützt. Andere CD-ROM-Erweiterungen funktionieren ggf. jedoch auch.

2. Öffnen Sie eine KVM-Sitzung mit dem entsprechenden Zielserver.
   a. Rufen Sie über die Remotekonsole die Seite "Port Access" (Portzugriff) auf.
   b. Stellen Sie auf dieser Seite eine Verbindung mit dem Zielserver her:
   - Klicken Sie unter "Port Name" (Portname) auf den entsprechenden Server.
   - Wählen Sie im Menü "Port Action" (Portaktion) den Befehl "Connect" (Verbinden) aus. Der Zielserver wird in einem Fenster des Virtual KVM Client geöffnet.
3. Stellen Sie eine Verbindung mit dem virtuellen Medium her.



Virtuelles Medium	Entsprechende VM-Option
Lokale Laufwerke	Local Drives (Lokale Laufwerke)
Lokale CD-/DVD-Laufwerke	CD-ROM-/DVD-ROM-/ISO-Abbilder
ISO-Abbilder	Connect CD-ROM/ISO Image (CD-ROM-/ISO-Abbild verbinden)
Dateiserver-ISO-Abbilder	Connect CD-ROM/ISO Image (CD-ROM-/ISO-Abbild verbinden)

Nach Abschluss Ihrer Aufgaben trennen Sie die Verbindung zum virtuellen Medium. Siehe ***Trennen von virtuellen Medien*** (auf Seite 117)

Dateiserver-Setup (nur für Dateiserver-ISO-Abbilder)

Hinweis: Dieses Feature ist nur für den Zugriff auf Dateiserver-ISO-Abbilder über virtuelle Medien erforderlich.

Das ISO9660-Format wird standardmäßig von Raritan unterstützt. Andere CD-ROM-Erweiterungen funktionieren ggf. jedoch auch.

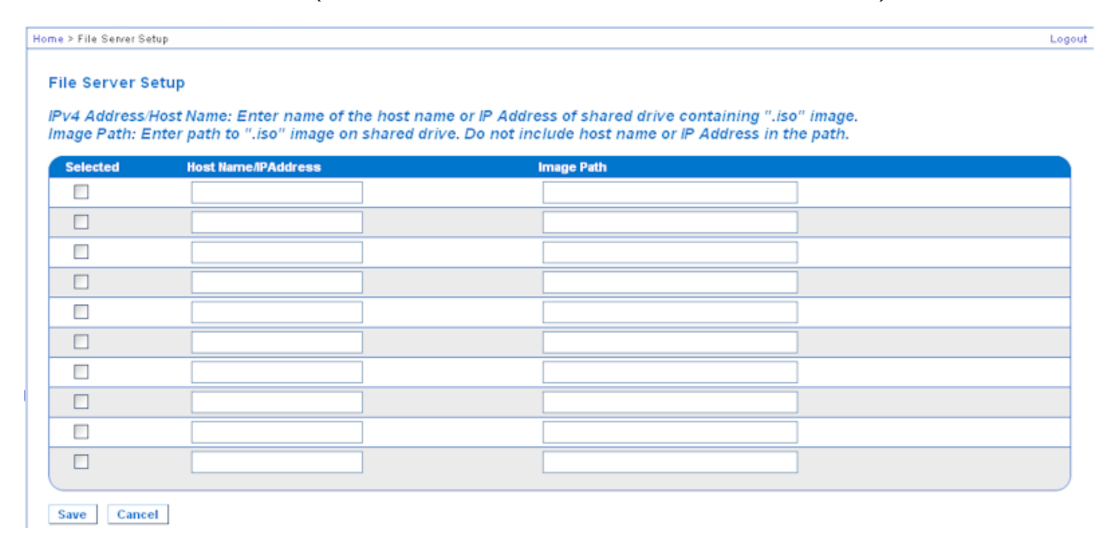
Legen Sie auf der Seite "File Server Setup" (Dateiserver-Setup) der Remotekonsole die Dateiserver und Abbildpfade fest, auf die Sie über virtuelle Medien zugreifen möchten. Hier angegebene Dateiserver-ISO-Abbilder stehen im Dialogfenster "Map Virtual Media CD/ISO Image" (CD-/ISO-Abbild als virtuelles Medium zuordnen) unter "Remote Server ISO Image" (ISO-Abbild auf Remoteserver) in den Dropdownlisten "Hostname" und "Image" (Abbild) zur Auswahl. Siehe **CD-ROM-/DVD-ROM-/ISO-Abbilder** (auf Seite 115).

So legen Sie Dateiserver-ISO-Abbilder für den virtuellen Medienzugriff fest:

1. Wählen Sie in der Remotekonsole "Virtual Media" (Virtuelle Medien) aus. Die Seite "File Server Setup" (Dateiserver-Setup) wird angezeigt.
2. Aktivieren Sie das Kontrollkästchen "Selected" (Ausgewählt) für alle Medien, die als virtuelle Medien zugänglich sein sollen.
3. Geben Sie Informationen zu den Dateiserver-ISO-Abbildern ein, auf die Sie zugreifen möchten:
   - IP Address/Host Name (IP-Adresse/Hostname) – Hostname oder IP-Adresse des Dateiservers.
   - Image Path (Abbildpfad) – Vollständiger Pfad zum Speicherort des ISO-Abbildes.

Hinweis: Der Hostname darf aus maximal 232 Zeichen bestehen.

4. Klicken Sie auf "Save" (Speichern). Alle hier angegebenen Medien stehen nun im Dialogfeld "Map Virtual Media CD/ISO Image" (CD-/ISO-Abbild als virtuelles Medium zuordnen) zur Auswahl.



Hinweis: Aufgrund von technischen Einschränkungen der Drittanbieter-Software des KX2 können Sie bei Verwendung einer IPv6-Adresse nicht über virtuelle Medien auf ein Remote-ISO-Abbild zugreifen.

Hinweis: Wenn Sie eine Verbindung zu einen Windows 2003-Server herstellen und versuchen, ein ISO-Abbild vom Server zu laden, ist es möglich, dass Sie die Fehlermeldung "Virtual Media mounting on port failed. Unable to connect to the file server or incorrect File Server username and password". (Installation der virtuellen Medien auf Port fehlgeschlagen. Verbindung mit Dateiserver konnte nicht hergestellt werden oder falsches Kennwort bzw. falschen Benutzernamen für Dateiserver verwendet.) angezeigt bekommen. Falls dies eintritt, deaktivieren Sie unter den Richtlinien für den Dömänen-Controller die Option "Microsoft Network Server: Digitally Sign Communications" (Microsoft-Netzwerk [Server]: Kommunikation digital signieren).



Herstellen einer Verbindung mit virtuellen Medien

Local Drives (Lokale Laufwerke)

Mit dieser Option installieren Sie ein gesamtes Laufwerk. Das gesamte Festplattenlaufwerk wird auf dem Zielserver virtuell installiert. Verwenden Sie diese Option nur für Festplatten und externe Laufwerke. Netzwerklaufwerke, CD-ROM- oder DVD-ROM-Laufwerke sind nicht enthalten. Nur für diese Option ist "Read/Write" (Lese-/Schreibzugriff) verfügbar.

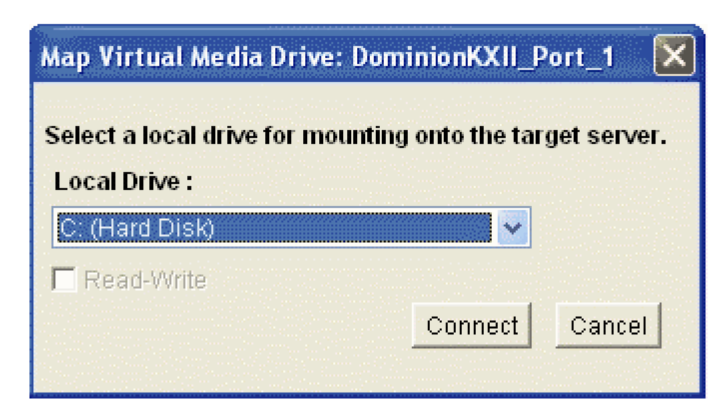
Hinweis: KVM-Zielserver mit bestimmten Versionen des Windows-Betriebssystems akzeptieren möglicherweise keine neuen Massenspeicherverbindungen, nachdem eine NTFS-formatierte Partition (z. B. das lokale Laufwerk C) an sie umgeleitet wurde.

Schließen Sie in diesem Fall die Remotekonsole, und stellen Sie erneut eine Verbindung her, bevor Sie ein weiteres virtuelles Mediengerät umleiten. Wenn andere Benutzer mit demselben Zielserver verbunden sind, müssen auch sie diese Verbindung trennen.

Hinweis: Mounten Sie beim Dominion KX II 2.1.0 und höher ein externes Laufwerk, z. B. ein Diskettenlaufwerk, so leuchtet die LED permanent, da das Gerät alle 500 Millisekunden prüft, ob das Laufwerk noch installiert ist.

So greifen Sie auf ein Laufwerk auf dem Clientcomputer zu:

1. Wählen Sie im Virtual KVM Client "Virtual Media" > "Connect Drive" (Virtuelle Medien > Laufwerk verbinden) aus. Das Dialogfeld "Map Virtual Media Drive" (Virtuelles Medienlaufwerk zuordnen) wird angezeigt.



2. Wählen Sie das entsprechende Laufwerk in der Dropdownliste "Local Drive" (Lokales Laufwerk) aus.

3. Für den Lese- und Schreibzugriff müssen Sie das Kontrollkästchen "Read-Write" (Lese-/Schreibzugriff) aktivieren. Diese Option steht nur für Wechsellaufwerke zur Verfügung. Weitere Informationen finden Sie unter ***Fälle, in denen Lese-/Schreibzugriff nicht verfügbar ist*** (auf Seite 114). Bei dieser Option können Sie Daten auf dem angeschlossenen USB-Datenträger lesen und schreiben.

   WARNUNG: Den Lese-/Schreibzugriff zu aktivieren kann gefährlich sein! Wenn mehrere Einheiten gleichzeitig auf dasselbe Laufwerk zugreifen, kann dies zu Datenbeschädigungen führen. Sollten Sie den Schreibzugriff nicht benötigen, deaktivieren Sie dieses Kontrollkästchen.

4. Klicken Sie auf "Connect" (Verbinden). Das Medium wird auf dem Zielserver virtuell installiert. Sie können darauf wie auf jedes andere Laufwerk zugreifen.

Fälle, in denen Lese-/Schreibzugriff nicht verfügbar ist

Der Lese-/Schreibzugriff auf virtuelle Medien ist in den folgenden Situationen nicht verfügbar:

- Bei allen Festplatten
- Wenn das Laufwerk schreibgeschützt ist.
- Wenn der Benutzer nicht über eine Lese-/Schreibberechtigung verfügt.
  - Wenn unter "Port Permission" (Portberechtigung) für "Access" (Zugriff) die Einstellung "None" (Kein) oder "View" (Ansehen) ausgewählt ist.
  - Wenn unter "Port Permission" (Portberechtigung) für "VM Access" (VM-Zugriff) die Einstellung "Read-Only" (Schreibgeschützt) oder "Deny" (Ablehnen) ausgewählt ist.



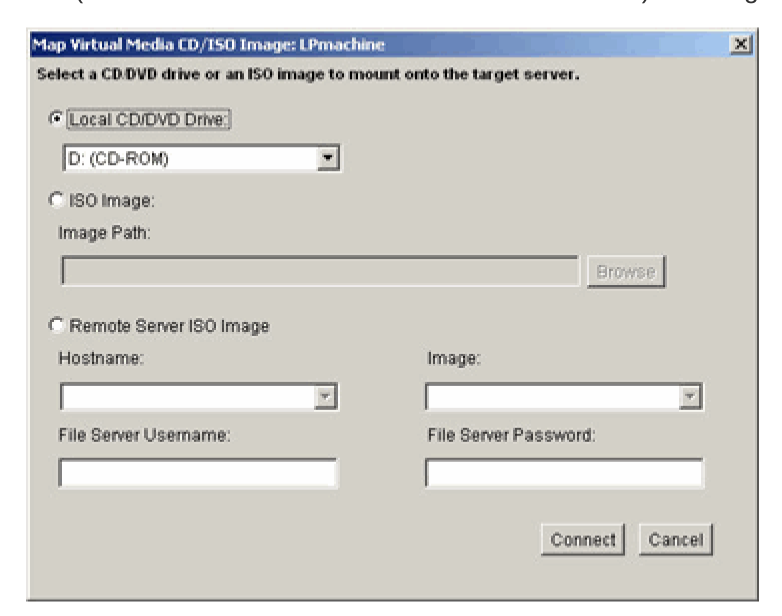
CD-ROM-/DVD-ROM-/ISO-Abbilder

Mit dieser Option installieren Sie CD-ROM-, DVD-ROM- und ISO-Abbilder.

Hinweis: Das ISO9660-Format wird standardmäßig von Raritan unterstützt. Andere CD-ROM-Erweiterungen funktionieren ggf. jedoch auch.

▶ So greifen Sie auf ein CD-ROM-, DVD-ROM- oder ISO-Abbild zu:

1. Wählen Sie im Virtual KVM Client "Virtual Media" > "Connect CD-ROM/ISO Image" (Virtuelle Medien > CD-ROM-/ISO-Abbild verbinden) aus. Das Dialogfeld "Map Virtual Media CD/ISO Image" (CD-/ISO-Abbild als virtuelles Medium zuordnen) wird angezeigt.



2. Gehen Sie bei internen und externen CD-ROM- und DVD-ROM-Laufwerken folgendermaßen vor:
   a. Wählen Sie die Option "Local CD/DVD Drive" (Lokales CD-/DVD-Laufwerk) aus.
   b. Wählen Sie das entsprechende Laufwerk in der Dropdownliste "Local CD/DVD Drive" (Lokales CD-/DVD-Laufwerk) aus. Diese Liste enthält alle verfügbaren internen und externen CD- und DVD-Laufwerksnamen.
   c. Klicken Sie auf "Connect" (Verbinden).
3. Gehen Sie bei ISO-Abbildern folgendermaßen vor:
   a. Wählen Sie die Option "ISO Image" (ISO-Abbild). Mit dieser Option greifen Sie auf ein Laufwerkabbild einer CD, DVD oder Festplatte zu. Nur das ISO-Format wird unterstützt.

   b. Klicken Sie auf die Schaltfläche "Browse" (Durchsuchen).
   c. Navigieren Sie zu dem Pfad des gewünschten Laufwerkabbilds, und klicken Sie auf "Open" (Öffnen). Der Pfad wird in das Feld "Image Path" (Abbildpfad) geladen.
   d. Klicken Sie auf "Connect" (Verbinden).

4. Gehen Sie bei Remote-ISO-Abbildern auf einem Dateiserver folgendermaßen vor:
   a. Wählen Sie die Option "Remote Server ISO Image" (ISO-Abbild auf Remoteserver) aus.
   b. Wählen Sie in der Dropdown-Liste einen Hostnamen und ein Abbild aus. Zur Verfügung stehen die Dateiserver und Abbildpfade, die Sie auf der Seite "File Server Setup" (Dateiserver-Setup) konfiguriert haben. Die Dropdown-Liste enthält nur Elemente, die Sie auf der Seite "File Server Setup" (Dateiserver-Setup) konfiguriert haben.
   c. File Server Username (Dateiserver-Benutzername) – Der für den Zugriff auf den Dateiserver erforderliche Benutzername.
   d. File Server Password (Dateiserver-Kennwort) – Das für den Zugriff auf den Dateiserver erforderliche Kennwort (Eingabe erfolgt verdeckt).
   e. Klicken Sie auf "Connect" (Verbinden).

   Das Medium wird auf dem Zielserver virtuell installiert. Sie können darauf wie auf jedes andere Laufwerk zugreifen.

Hinweis: Wenn Sie Dateien auf einem Linux-Zielgerät bearbeiten, verwenden Sie den Befehl "Linux Sync" (Linux-Synchronisierung), nachdem die Dateien mithilfe eines virtuellen Mediums kopiert wurden, um die kopierten Dateien anzuzeigen. Die Dateien werden möglicherweise erst angezeigt, nachdem die Synchronisierung durchgeführt wurde.

Hinweis: Wenn Sie mit Windows 7 arbeiten werden Wechseldatenträger nicht standardmäßig im Windows-Ordner "Arbeitsplatz" angezeigt, sobald Sie ein lokales CD-/DVD-Laufwerk oder ein lokales oder Remote-ISO-Abbild mounten. Um das lokale CD-/DVD-Laufwerk oder das lokale oder Remote-ISO-Abbild in diesem Ordner anzuzeigen, wählen Sie "Extras" > "Ordneroptionen" > "Ansicht" aus und deaktivieren die Option "Leere Laufwerke im Ordner "Computer" ausblenden".

Hinweis: Aufgrund von technischen Einschränkungen der Drittanbieter-Software des KX2 können Sie bei Verwendung einer IPv6-Adresse nicht über virtuelle Medien auf ein Remote-ISO-Abbild zugreifen.



Trennen von virtuellen Medien

So trennen Sie virtuelle Medienlaufwerke:

- Wählen Sie für lokale Laufwerke "Virtual Media" > "Disconnect Drive" (Virtuelle Medien > Laufwerk trennen) aus.
- Wählen Sie für CD-ROM-, DVD-ROM- und ISO-Abbilder "Virtual Media > Disconnect CD-ROM/ISO Image" (Virtuelle Medien > CD-ROM-/ISO-Abbild trennen) aus.

Hinweis: Anstatt das virtuelle Medium über den Befehl "Disconnect" (Trennen) zu trennen, können Sie auch einfach die KVM-Verbindung beenden.

Kapitel 6 USB-Profile

In diesem Kapitel

Überblick

Um die Kompatibilität des Dominion KX II auf verschiedene KVM-Zielserver auszuweiten, bietet Raritan eine Standardauswahl an USB-Konfigurationsprofilen für die Implementierung auf vielen Betriebssystemen und Servern auf BIOS-Ebene an.

Das generische USB-Profil (Standard) erfüllt die Anforderungen der großen Mehrheit der bereitgestellten KVM-Zielserverkonfigurationen. Weitere Profile stehen zur Verfügung, um die speziellen Anforderungen anderer häufig bereitgestellten Serverkonfigurationen (z. B. Linux® und Mac OS X®) zu erfüllen. Außerdem stehen einige Profile (festgelegt nach Plattformname und BIOS-Revision) zur Verfügung, um die Kompatibilität der Funktion der virtuellen Medien mit dem Zielserver zu verbessern (wenn z. B. auf BIOS-Ebene gearbeitet wird).

USB-Profile werden unter "Device Settings" > "Port Configuration" > "Port" (Geräteeinstellungen > Portkonfiguration > Port) auf den lokalen und Remotekonsolen des Dominion KX II konfiguriert. Ein Geräteadministrator kann den Port mit den Profilen konfigurieren, die den Anforderungen des Benutzers und der Zielserverkonfiguration am besten entsprechen.

Ein Benutzer, der eine Verbindung mit einem KVM-Zielserver herstellt, kann unter diesen vordefinierten Profilen im ***Virtual KVM Client*** (auf Seite 63) wählen, je nach Betriebsstatus des KVM-Zielservers. Wenn beispielsweise der Server ausgeführt wird und der Benutzer das Windows®-Betriebssystem verwenden möchte, ist es sinnvoll, das generische Profil zu verwenden. Wenn der Benutzer jedoch die Einstellungen im BIOS-Menü ändern oder von einem virtuellen Medienlaufwerk einen Neustart ausführen möchte, kann, je nach Zielservermodell, ein BIOS-Profil eher geeignet sein.

Sollte keines der von Raritan bereitgestellten Standard-USB-Profile mit dem betreffenden KVM-Zielgerät funktionieren, wenden Sie sich an den technischen Kundendienst von Raritan.



CIM-Kompatibilität

Um USB-Profile nutzen zu können, müssen Sie ein D2CIM-VUSB oder ein D2CIM-DVUSB mit aktualisierter Firmware verwenden. Ein VM-CIM ohne aktualisierte Firmware unterstützt eine große Anzahl an Konfigurationen (Tastatur, Maus, CD-ROM und Wechsellaufwerk), kann jedoch nicht die für bestimmte Zielkonfigurationen optimierten Profile nutzen. Daher sollten bestehende VM-CIMs mit der neuesten Firmware aktualisiert werden, um auf USB-Profile zugreifen zu können. Solange bestehende VM-CIMs noch nicht aktualisiert wurden, verfügen sie über eine Funktionalität, die dem generischen Profil entspricht.

VM-CIM-Firmware wird während einer Dominion KX II-Firmwareaktualisierung automatisch aktualisiert; VM-CIMs, die nicht über die aktuelle Firmware verfügen, können jedoch, wie unter ***Aktualisieren von CIMs*** (auf Seite 258) beschrieben, aktualisiert werden.

Weitere Informationen finden Sie unter ***Computer Interface Modules (CIMs)*** (auf Seite 307).

Verfügbare USB-Profile

Die aktuellen Version des Dominion KX II verfügt über eine Auswahl an USB-Profilen, die in der folgenden Tabelle beschrieben werden. Neue Profile sind in jeder von Raritan zur Verfügung gestellten Firmwareaktualisierung enthalten. Wenn neue Profile hinzugefügt werden, werden diese in der Hilfe dokumentiert.

USB-Profil	Beschreibung
BIOS Dell® PowerEdge® 1950/2950/2970/6950/R200	Dell PowerEdge 1950/2950/2970/6950/R200-BIOS Verwenden Sie entweder dieses oder das generische Profil für das Dell PowerEdge 1950/2950/2970/6950/R200-BIOS. Einschränkungen: • Keine
BIOS DellOptiplex Keyboard Only	Dell Optiplex BIOS Access (Nur Tastatur) Verwenden Sie dieses Profil, um Tastaturfunktionalität für das Dell Optiplex-BIOS zu erhalten, wenn das D2CIM-VUSB verwendet wird. Verwenden Sie bei Nutzung des neuen D2CIM-DVUSB das generische Profil.



<table>
<tr><th>USB-Profil</th><th>Beschreibung</th></tr>
<tr><td></td><td>Hinweis:
Optiplex 210L/280/745/GX620 benötigt das D2CIM-DVUSB mit generischem Profil, um virtuelle Medien zu unterstützen.
Einschränkungen:
USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s)
Keine Unterstützung für virtuelle Medien</td></tr>
<tr><td>BIOS DellPowerEdge Keyboard Only</td><td>Dell PowerEdge BIOS Access (Nur Tastatur)

Verwenden Sie dieses Profil, um Tastaturfunktionalität für das Dell PowerEdge-BIOS zu erhalten, wenn das D2CIM-VUSB verwendet wird. Verwenden Sie bei Nutzung des neuen D2CIM-DVUSB das generische Profil.

Hinweis:
PowerEdge 650/1650/1750/2600/2650 BIOS unterstützen keine USB-, CD-ROM-Laufwerke und Festplatten als startbares Gerät.
PowerEdge 750/850/860/1850/2850/SC1425-BIOS benötigt das D2CIM-DVUSB mit generischem Profil, um virtuelle Medien zu unterstützen.
Verwenden Sie das Profil "BIOS Dell PowerEdge 1950/2950/2970/6950/R200" oder das generische Profil für PowerEdge 1950/2950/2970/6950/R200, wenn im BIOS gearbeitet wird.
Einschränkungen:
USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s)
Absolute Mouse Synchronization™ (Absolute Maussynchronisierung)</td></tr>
</table>



USB-Profil	Beschreibung
	nicht unterstützt • Keine Unterstützung für virtuelle Medien
BIOS Generic	BIOS Generic Verwenden Sie dieses Profil, wenn das generische Profil des Betriebssystems auf dem BIOS nicht funktioniert. WARNUNG: Die USB-Erkennung wird gestartet, wenn virtuelle Medien verbunden oder getrennt werden. Einschränkungen: • USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s) • Absolute Mouse Synchronization™ (Absolute Maussynchronisierung) nicht unterstützt • Virtuelle CD-ROM-Laufwerke und Plattenlaufwerke können nicht gleichzeitig verwendet werden.
BIOS HP® Proliant™ DL145	HP Proliant DL145 PhoenixBIOS Verwenden Sie dieses Profil für HP Proliant DL145 PhoenixBIOS während der Installation des Betriebssystems. Einschränkungen: • USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s)
BIOS HP Compaq® DC7100/DC7600	BIOS HP Compaq DC7100/DC7600 Verwenden Sie dieses Profil zum Hochfahren von Desktops der Serie "HP Compaq DC7100/DC7600" über virtuelle Medien. Einschränkungen: • Virtuelle CD-ROM-Laufwerke und Plattenlaufwerke können nicht gleichzeitig verwendet werden.
BIOS IBM ThinkCentre Lenovo	IBM Thinkcentre Lenovo BIOS

USB-Profil	Beschreibung
	Verwenden Sie dieses Profil für die IBM® Thinkcentre Lenovo-Hauptplatine (Modell 828841U) bei BIOS-Vorgängen. Einschränkungen: • USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s) • Virtuelle CD-ROM-Laufwerke und Plattenlaufwerke können nicht gleichzeitig verwendet werden.
BIOS Lenovo ThinkPad T61 & X61	BIOS Lenovo ThinkPad T61 und X61 (Hochfahren über virtuelle Medien) Verwenden Sie dieses Profil zum Hochfahren von Laptops der Serie T61 und X61 über virtuelle Medien. Einschränkungen: • USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s)
BIOS Mac	BIOS Mac Verwenden Sie dieses Profil für Mac®-BIOS. Einschränkungen: • Absolute Mouse Synchronization™ (Absolute Maussynchronisierung) nicht unterstützt • Virtuelle CD-ROM-Laufwerke und Plattenlaufwerke können nicht gleichzeitig verwendet werden.
Generisch	Das generische USB-Profil entspricht in etwa dem Verhalten der ursprünglichen KX2-Version. Verwenden Sie dies für die Betriebssysteme Windows 2000®, Windows XP®, Windows Vista® und höher. Einschränkungen: • Keine
HP Proliant DL360/DL380 G4	HP Proliant DL360/DL380 G4 (HP



USB-Profil	Beschreibung
(HP SmartStart CD)	SmartStart CD) Verwenden Sie dieses Profil für den Server der Serie "HP Proliant DL360/DL380 G4" bei der Installation des Betriebssystems unter Verwendung der HP SmartStart CD. Einschränkungen: • USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s) • Absolute Mouse Synchronization™ (Absolute Maussynchronisierung) nicht unterstützt
HP Proliant DL360/DL380 G4 (Windows 2003® Server-Installation)	HP Proliant DL360/DL380 G4 (Windows 2003 Server-Installation) Verwenden Sie dieses Profil für den Server der Serie "HP Proliant DL360/DL380 G4" bei der Installation von Windows 2003 Server ohne Verwendung der HP SmartStart CD. Einschränkungen: • USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s)
Linux®	Generisches Linux-Profil Dies ist das generische Linux-Profil. Verwenden Sie es für Redhat Enterprise Linux, SuSE Linux Enterprise Desktop und ähnliche Distributionen. Einschränkungen: • Absolute Mouse Synchronization™ (Absolute Maussynchronisierung) nicht unterstützt
MAC OS X® (10.4.9 und höher)	Mac OS-X, Version 10.4.9 und höher Dieses Profil kompensiert die Skalierung von Mauskoordination, die in den neueren Versionen von Mac OS-X eingeführt wurden. Wählen Sie dieses Profil aus, wenn die lokalen und Remote-Mauspositionen an den Desktop-Rändern nicht mehr

USB-Profil	Beschreibung
	synchronisiert sind. Einschränkungen: • Virtuelle CD-ROM-Laufwerke und Plattenlaufwerke können nicht gleichzeitig verwendet werden.
RUBY Industrial Mainboard (AwardBIOS)	RUBY Industrial Mainboard (AwardBIOS) Verwenden Sie dieses Profil für die Industriemainboards der Serie "RUBY-9715VG2A" mit Phoenix/AwardBIOS v6.00PG. Einschränkungen: • USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s) • Virtuelle CD-ROM-Laufwerke und Plattenlaufwerke können nicht gleichzeitig verwendet werden.
Supermicro Mainboard Phoenix (AwardBIOS)	Supermicro Mainboard Phoenix AwardBIOS Verwenden Sie diese Profil für Hauptplatinen der Serie "Supermicro" mit Phoenix AwardBIOS. Einschränkungen: • Virtuelle CD-ROM-Laufwerke und Plattenlaufwerke können nicht gleichzeitig verwendet werden.
Suse 9.2	SuSE Linux 9.2 Verwenden Sie dieses Profil für die SuSE Linux 9.2-Distribution. Einschränkungen: • Absolute Mouse Synchronization™ (Absolute Maussynchronisierung) nicht unterstützt • USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s)
Troubleshooting 1	Fehlerbehebungsprofil 1 • Massenspeicher vorrangig



USB-Profil	Beschreibung
	• Tastatur und Maus (Typ 1) • USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s) • Virtuelle CD-ROM-Laufwerke und Plattenlaufwerke können nicht gleichzeitig verwendet werden. WARNUNG: Die USB-Erkennung wird gestartet, wenn virtuelle Medien verbunden oder getrennt werden.
Troubleshooting 2	Fehlerbehebungsprofil 2 • Tastatur und Maus (Typ 2) vorrangig • Massenspeicher • USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s) • Virtuelle CD-ROM-Laufwerke und Plattenlaufwerke können nicht gleichzeitig verwendet werden. WARNUNG: Die USB-Erkennung wird gestartet, wenn virtuelle Medien verbunden oder getrennt werden.
Troubleshooting 3	Fehlerbehebungsprofil 3 • Massenspeicher vorrangig • Tastatur und Maus (Typ 2) • USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s) • Virtuelle CD-ROM-Laufwerke und Plattenlaufwerke können nicht gleichzeitig verwendet werden. WARNUNG: Die USB-Erkennung wird gestartet, wenn virtuelle Medien verbunden oder getrennt werden.



USB-Profil	Beschreibung
Use Full Speed for Virtual Media CIM (Volle Geschwindigkeit für virtuelles Medien-CIM verwenden)	Use Full Speed for Virtual Media CIM (Volle Geschwindigkeit für virtuelles Medien-CIM verwenden) Dieses Profil entspricht in etwa dem Verhalten der ursprünglichen KX2-Version, wenn die Option "Full Speed for Virtual Media CIM" (Volle Geschwindigkeit für virtuelles Medien-CIM) aktiviert ist. Hilfreich bei einem BIOS, das nicht mit Hochgeschwindigkeits-USB-Geräten funktioniert. Einschränkungen: • USB-Busgeschwindigkeit beschränkt auf volle Geschwindigkeit (12 Mbit/s)

Auswählen von Profilen für einen KVM-Port

Dominion KX II enthält eine Reihe von USB-Profilen, die Sie einem KVM-Port zuweisen können, basierend auf den Eigenschaften des KVM-Zielservers, mit dem das Profil verbunden wird. Sie können USB-Profile unter "Device Settings" > "Port Configuration" > "Port" (Geräteeinstellungen > Portkonfiguration > Port) auf der lokalen oder der Remotekonsole des Dominion KX II einem KVM-Port zuweisen.

Der Administrator legt die Profile fest, die am wahrscheinlichsten für ein spezielles Zielgerät benötigt werden. Diese Profile stehen anschließend über MPC/VKC zur Auswahl bereit. Wenn ein Profil nicht zur Verwendung freigegeben wurde, können sie auf alle verfügbaren Profile zugreifen, indem Sie "USB Profile" > "Other Profiles" (USB-Profil > Weitere Profile) auswählen.

Durch die Zuordnung von USB-Profilen zu einem KVM-Port sind diese Profile für Benutzer, die mit einem KVM-Zielserver verbunden sind, verfügbar. Wenn erforderlich, kann der Benutzer ein USB-Profil aus dem USB-Profilmenü im VKC oder MPC auswählen.

Informationen zur Zuordnung von USB-Profilen zu einem KVM-Port finden Sie unter ***Konfigurieren von USB-Profilen (Seite "Port")*** (auf Seite 222).



Mausmodi bei Verwendung des Mac OS-X-USB-Profils mit einem DCIM-VUSB.

Wenn Sie ein DCIM-VUSB mit einem Mac OS-X®-USB-Profil verwenden und Mac OS-X 10.4.9 (oder höher) ausführen, muss beim Neustart der Modus "Single Mouse" (Ein Cursor) ausgewählt sein, um die Maus im Menü "Boot" zu verwenden.

So konfigurieren Sie die Maus für das Arbeiten im Menü "Boot":

1. Starten Sie Ihren Mac-Computer, und drücken Sie die Alt-Taste, um das Menü "Boot" zu öffnen. Zu diesem Zeitpunkt reagiert die Maus noch nicht.
2. Wählen Sie den Mausmodus "Intelligent" und anschließend den Mausmodus "Single Mouse" (Ein Cursor) aus. Jetzt reagiert die Maus.

   Hinweis: Im Modus "Single Mouse" (Ein Cursor) ist die Geschwindigkeit des Mauszeigers möglicherweise gering.

3. Sobald Sie das Menü "Boot" verlassen haben und das Betriebssystem hochgefahren ist, beenden Sie den Modus "Single Mouse" (Ein Cursor), und schalten Sie zurück in den Mausmodus "Absolute Mouse" (Absolut), um eine bessere Leistung der Maus zu erhalten.



Kapitel 7 User Management (Benutzerverwaltung)

In diesem Kapitel

Benutzergruppen

Dominion KX II speichert eine interne Liste aller Benutzer- und Gruppennamen, um die Zugriffsautorisierung und die Berechtigungen festzulegen. Diese Informationen werden intern in einem verschlüsselten Format gespeichert. Es gibt verschiedene Arten der Authentifizierung. Diese wird als lokale Authentifizierung bezeichnet. Alle Benutzer müssen authentifiziert werden. Wenn Dominion KX II für LDAP/LDAPS oder RADIUS konfiguriert wurde, wird erst deren entsprechende Authentifizierung durchgeführt und anschließend die lokale Authentifizierung.

Jedes Dominion KX II enthält standardmäßig drei Benutzergruppen. Diese Gruppen können nicht gelöscht werden:

Benutzer	Beschreibung
Admin	Benutzer dieser Gruppe verfügen über vollständige Administratorrechte. Der ursprüngliche werkseitige Standardbenutzer ist Mitglied dieser Gruppe und verfügt über sämtliche Systemrechte. Außerdem muss der Benutzer "Admin" der Gruppe "Admin" angehören.
Unknown (Unbekannt)	Dies ist die Standardgruppe für Benutzer, die extern über LDAP/LDAPS oder RADIUS authentifiziert werden oder die im System unbekannt sind. Wenn der externe LDAP/LDAPS- oder RADIUS-Server keine gültige Benutzergruppe erkennt, wird die Gruppe "Unknown" (Unbekannt) verwendet. Außerdem wird jeder neu erstellte Benutzer automatisch in diese Gruppe aufgenommen, bis der Benutzer einer anderen Gruppe zugewiesen wird.
Individual Group (Individuelle Gruppe)	Eine individuelle Gruppe ist im Prinzip eine aus einer Person bestehende "Gruppe". Dies bedeutet, dass sich der Benutzer in seiner eigenen Gruppe befindet und nicht mit anderen echten Gruppen verknüpft ist. Individuelle Gruppen können Sie am @-Zeichen im Gruppennamen erkennen. In individuellen Gruppen

	können Benutzerkonten dieselben Rechte wie eine Gruppe aufweisen.

In Dominion KX II können bis zu 254 Benutzergruppen erstellt werden.

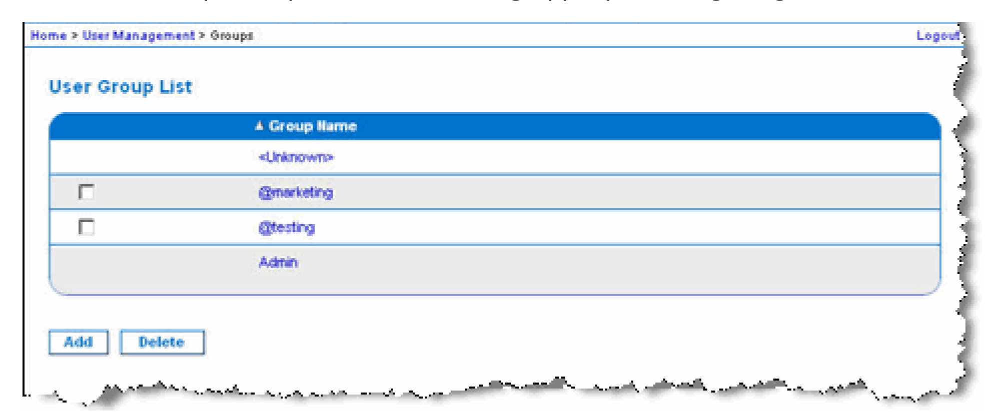
User Group List (Liste der Benutzergruppen)

Benutzergruppen werden bei der lokalen und der Remoteauthentifizierung (über RADIUS oder LDAP/LDAPS) verwendet. Es ist empfehlenswert, Benutzergruppen vor dem Erstellen einzelner Benutzer zu definieren, da jeder Benutzer einer vorhandenen Benutzergruppe hinzugefügt werden muss.

Die Seite "User Group List" (Liste der Benutzergruppen) enthält eine Liste aller Benutzergruppen, die in auf- oder absteigender Reihenfolge sortiert werden kann, indem Sie auf die Spaltenüberschrift "Group Name" (Gruppenname) klicken. Auf der Seite "User Group List" (Liste der Benutzergruppen) können Sie außerdem Benutzergruppen hinzufügen, ändern oder löschen.

So zeigen Sie eine Liste der Benutzergruppen an:

- Wählen Sie "User Management" > "User Group List" (Benutzerverwaltung > Liste der Benutzergruppen) aus. Die Seite "User Group List" (Liste der Benutzergruppen) wird angezeigt.





Beziehung zwischen Benutzern und Gruppen

Benutzer sind Mitglied in einer Gruppe, und Gruppen verfügen über bestimmte Berechtigungen. Sie können Zeit sparen, indem Sie die verschiedenen Benutzer Ihrer Dominion KX II-Einheit in Gruppen organisieren. So können Sie die Berechtigungen aller Benutzer in einer Gruppe auf einmal verwalten anstatt für jeden Benutzer einzeln.

Sie können bei Bedarf auch darauf verzichten, bestimmte Benutzer Gruppen zuzuordnen. In diesem Fall können Sie den Benutzer als "Individuell" klassifizieren.

Nach der erfolgreichen Authentifizierung verwendet das Gerät Gruppeninformationen, um die Berechtigungen des Benutzers zu bestimmen, z. B. die Zugriffsberechtigungen für verschiedene Server-Ports, ob ein Neustart des Geräts zulässig ist und weitere Funktionen.

Hinzufügen einer neuen Benutzergruppe

So fügen Sie eine neue Benutzergruppe hinzu:

1. Öffnen Sie die Seite "Group" (Gruppe), indem Sie "User Management" > "Add New User Group" (Benutzerverwaltung > Neue Benutzergruppe hinzufügen) auswählen oder auf der Seite "User Group List" (Liste der Benutzergruppen) auf die Schaltfläche "Add" (Hinzufügen) klicken.

   Die Seite "Group" (Gruppe) umfasst die folgenden Kategorien: Group (Gruppe), Permissions (Berechtigungen), Port Permissions (Portberechtigungen) und IP ACL (IP-ACL).

2. Geben Sie im Feld "Group Name" (Gruppenname) einen aussagekräftigen Namen für die neue Benutzergruppe ein (bis zu 64 Zeichen).
3. Legen Sie unter "Permissions" (Berechtigungen) die Berechtigungen für die Gruppe fest. Aktivieren Sie die Kontrollkästchen für die Berechtigungen, die Sie allen Benutzern in dieser Gruppe gewähren möchten. Siehe ***Festlegen von Berechtigungen*** (auf Seite 133).
4. Legen Sie unter "Port Permissions" (Portberechtigungen) die Portberechtigungen fest. Legen Sie die für die Benutzer in dieser Gruppe zugänglichen Serverports fest, und geben Sie den Zugriffstyp an. Siehe ***Festlegen von Portberechtigungen*** (auf Seite 135).
5. Legen Sie die IP-ACL fest. Mit diesem Feature beschränken Sie den Zugriff auf das Dominion KX II-Gerät, indem Sie IP-Adressen angeben. Dies gilt nur für Benutzer einer bestimmten Gruppe, im Gegensatz zur IP-Zugriffssteuerung, die für alle Zugriffsversuche auf das Gerät gilt und Priorität hat. **Optional**. Siehe ***Gruppenbasierte IP-ACL (IP-Zugriffssteuerungsliste)*** (auf Seite 137).



6. Klicken Sie auf OK.

Hinweis: Im MPC und auf der lokalen Dominion KX II-Konsole sind viele administrative Funktionen verfügbar. Diese Funktionen stehen nur Mitgliedern der Standardgruppe "Admin" zur Verfügung.

Hinweis: Sowohl IPv4- als auch IPv6-Adressen werden unterstützt.



Home > User Management > Group

Group

Group Name *

▼ Permissions

- ☑ Device Access While Under CC-SG Management
- ☑ Device Settings
- ☑ Diagnostics
- ☑ Maintenance
- ☑ Modem Access
- ☑ PC-Share
- ☑ Security
- ☑ User Management

▼ Port Permissions

Port	Access	VM Access	Power Control
1: BC_Port1_R8_from_KX	Deny	Deny	Deny
1-1: BC_Port1_Slot1_To_Local_Port	Deny	Deny	Deny
1-2: Blade_Chassis_Port1_Slot2	Deny	Deny	Deny
1-3: Blade_Chassis_Port1_Slot3	Deny	Deny	Deny
1-4: Blade_Chassis_Port1_Slot4	Deny	Deny	Deny
1-5: Blade_Chassis_Port1_Slot5	Deny	Deny	Deny
1-6: Blade_Chassis_Port1_Slot6	Deny	Deny	Deny
1-7: Blade_Chassis_Port1_Slot7	Deny	Deny	Deny
1-8: Blade_Chassis_Port1_Slot8	Deny	Deny	Deny
1-9: Blade_Chassis_Port1_Slot9	Deny	Deny	Deny
1-10: Blade_Chassis_Port1_Slot10	Deny	Deny	Deny
1-11: Blade_Chassis_Port1_Slot11	Deny	Deny	Deny
1-12: Blade_Chassis_Port1_Slot12	Deny	Deny	Deny
1-13: Blade_Chassis_Port1_Slot13	Deny	Deny	Deny
1-14: Blade_Chassis_Port1_Slot14	Deny	Deny	Deny
1-15: Blade_Chassis_Port1_Slot15	Deny	Deny	Deny
1-16: Blade_Chassis_Port1_Slot16	Deny	Deny	Deny
2: KX2_Port2_R9_from_CC	Deny	Deny	Deny
3: KX2_Port2_R9_from_CC	Deny	Deny	Deny
	☐ Set All to Deny	☐ Set All VM Access to Deny	☐ Set All Power to Deny
	☐ Set All to View	☐ Set All VM Access to Read-Only	
	☐ Set All to Control	☐ Set All VM Access to Read-Write	☐ Set All Power to Access

▼ IP ACL

Rule #	Starting IP	Ending IP	Action
			ACCEPT

Append | Insert | Replace | Delete

OK | Cancel

Festlegen von Berechtigungen

Wichtig: Wenn das Kontrollkästchen "User Management"



(Benutzerverwaltung) aktiviert ist, können Mitglieder der Gruppe die Berechtigungen aller Benutzer einschließlich ihrer eigenen ändern. Lassen Sie beim Zuordnen dieser Berechtigungen Vorsicht walten.

Berechtigung	Beschreibung
Gerätezugriff unter CC-SG-Verwaltung	Ermöglicht Benutzern und Benutzergruppen mit dieser Berechtigung den direkten Zugriff auf Dominion KX II unter Verwendung einer IP-Adresse, wenn die Option "Lokal Access" (Lokaler Zugriff) für das Gerät in CC-SG aktiviert ist. Es kann von der lokalen und der Remotekonsole sowie vom MPC, VKC und AKC auf das Gerät zugegriffen werden. Wird unter CC-SG-Verwaltung direkt auf ein Gerät zugegriffen, werden Zugriff und Verbindungsaktivitäten auf Dominion KX II protokolliert. Die Benutzerauthentifizierung erfolgt gemäß den Dominion KX II-Authentifizierungseinstellungen. *Hinweis: Die Benutzer der Gruppe "Admin" verfügen standardmäßig über diese Berechtigung.*
Device Settings (Geräteeinstellungen)	Netzwerkeinstellungen, Einstellungen für Datum und Uhrzeit, Portkonfiguration (Kanalnamen, Stromzuordnungen), Ereignisverwaltung (SNMP, Syslog), Dateiserver-Setups für virtuelle Medien
Diagnostics (Diagnose)	Status der Netzwerkschnittstelle, Netzwerkstatistik, Ping an den Host, Verfolgen der Route zum Host, Dominion KX II-Diagnose.
Wartung	Sichern und Wiederherstellen von Datenbanken, Firmware-Aktualisierung, Wiederherstellen der Standardeinstellungen, Neustart.
Modem Access (Modemzugriff)	Berechtigung zur Verwendung des Modems, um eine Verbindung zum Dominion KX II-Gerät herzustellen
PC-Share (PC-Freigabe)	Gleichzeitiger Zugriff auf ein Zielgerät durch mehrere Benutzer. Wenn Sie eine Schichtkonfiguration verwenden, in der ein Dominion KX II-Basisgerät für den Zugriff auf mehrere andere Schichtgeräte verwendet wird, müssen alle Geräte dieselben PC-Freigabeeinstellung



Berechtigung	Beschreibung
	verwenden. Weitere Informationen zu Schichten finden Sie unter ***Konfigurieren und Aktivieren von Schichten*** (auf Seite 167).
Sicherheit	SSL-Zertifikat, Sicherheitseinstellungen (VM-Freigabe, PC-Freigabe), IP-ACL.
User Management (Benutzerverwaltung)	Benutzer- und Gruppenverwaltung, Remoteauthentifizierung (LDAP/LDAPS/RADIUS), Anmeldeeinstellungen Wenn Sie eine Schichtkonfiguration verwenden, in der ein Dominion KX II-Basisgerät für den Zugriff auf mehrere andere Schichtgeräte verwendet wird, müssen auf allen Geräten dieselben Einstellungen für Benutzer, Benutzergruppe und Remote-Authentifizierung verwendet werden. Weitere Informationen zu Schichten finden Sie unter ***Konfigurieren und Aktivieren von Schichten*** (auf Seite 167).

Festlegen von Portberechtigungen

Sie können für jeden Serverport den Zugriffstyp der Gruppe sowie den Portzugriffstyp auf virtuelle Medien und die Stromzufuhrsteuerung festlegen. Die Standardeinstellung für alle Berechtigungen ist "Deny" (Ablehnen).

Portzugriff	
Option	**Beschreibung**
Deny (Ablehnen)	Zugriff vollständig verweigert
View (Ansehen)	Ansicht des Videobildes, aber keine Interaktion mit dem angeschlossenen Zielserver
Control (Steuern)	Steuerung des angeschlossenen Zielservers Die Option "Control" (Steuern) muss der Gruppe zugeordnet sein, wenn der Zugriff auf virtuelle Medien und Stromzufuhrsteuerung ebenso gewährt wird.



VM-Zugriff	
Option	**Beschreibung**
Deny (Ablehnen)	Berechtigung für virtuelle Medien wird für diesen Port vollständig verweigert
Read-Only (Lesezugriff)	Zugriff auf virtuelle Medien ist auf das Lesen beschränkt
Read-Write (Lese-/Schreib-zugriff)	Vollständiger Zugriff (Lesen und Schreiben) auf virtuelle Medien

Zugriff auf Stromzufuhrsteuerung	
Option	**Beschreibung**
Deny (Ablehnen)	Keine Berechtigung für die Stromzufuhrsteuerung auf dem Zielserver
Access (Zugriff)	Volle Berechtigung für die Stromzufuhrsteuerung auf einem Zielserver

Bei Blade-Chassis wird über die Berechtigungen zum Portzugriff der Zugriff auf die URLs, die für dieses Blade-Chassis konfiguriert wurden, gesteuert. Die verfügbaren Optionen lauten "Deny" (Ablehnen) oder "Control" (Steuern). Außerdem besitzt jedes Blade im Chassis eine eigene unabhängige Port-Berechtigungseinstellung.

Wenn Sie eine Schichtkonfiguration verwenden, in der ein Dominion KX II-Basisgerät für den Zugriff auf mehrere andere Schichtgeräte verwendet wird, erzwingt das Schichtgerät individuelle Portsteuerungsebenen. Weitere Informationen zu Schichten finden Sie unter ***Konfigurieren und Aktivieren von Schichten*** (auf Seite 167).

Festlegen von Berechtigungen für eine individuelle Gruppe

▶ So legen Sie Berechtigungen für eine individuelle Benutzergruppe fest:

1. Wählen Sie die gewünschte Gruppe aus der Liste der Gruppen aus. Individuelle Gruppen können Sie am @-Zeichen im Gruppennamen erkennen.
2. Klicken Sie auf den Gruppennamen. Die Seite "Group" (Gruppe) wird angezeigt.
3. Wählen Sie die gewünschten Berechtigungen aus.



4. Klicken Sie auf OK.

Hinweis: Informationen zu weiteren Einstellungen bei der Verwendung von "Alternate RADIUS Authentication" (Alternierende RADIUS-Authentifizierung) finden Sie unter Alternate RADIUS Authentication Settings.

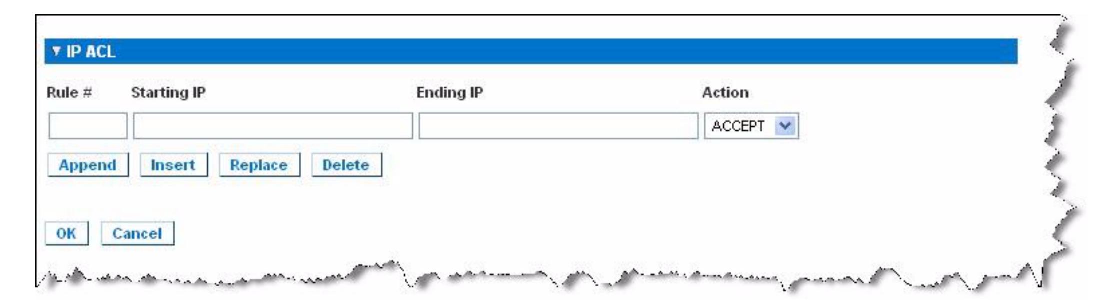
Gruppenbasierte IP-ACL (IP-Zugriffssteuerungsliste)

Wichtig: Gehen Sie bei der Verwendung der gruppenbasierten IP-Zugriffssteuerung bedachtsam vor. Der Zugriff auf Dominion KX II kann Ihnen verweigert werden, wenn sich Ihre IP-Adresse in einem Bereich befindet, der keine Zugriffsberechtigung hat.

Mit diesem Feature beschränken Sie den Zugriff auf das Dominion KX II-Gerät durch Benutzer in der ausgewählten Gruppe auf bestimmte IP-Adressen. Dies gilt nur für Benutzer einer bestimmten Gruppe, im Gegensatz zur IP-Zugriffssteuerung, die für alle Zugriffsversuche auf das Gerät gilt, zuerst verarbeitet wird und Priorität hat.

Wichtig: Die IP-Adresse 127.0.0.1 wird vom lokalen Dominion KX II-Port verwendet und kann nicht gesperrt werden.

Verwenden Sie den Abschnitt "IP ACL" (IP-ACL) auf der Seite "Group" (Gruppe), um Regeln für die IP-Zugriffssteuerung auf Gruppenebene hinzuzufügen, einzufügen, zu ersetzen und zu löschen.



So fügen Sie Regeln hinzu:

1. Geben Sie im Feld "Starting IP" (IP-Startadresse) die IP-Startadresse ein.
2. Geben Sie im Feld "Ending IP" (IP-Endadresse) die IP-Endadresse ein.
3. Wählen Sie unter "Action" (Aktion) eine der folgenden Optionen:
   - Accept (Akzeptieren) – Diese IP-Adressen können auf das Dominion KX II-Gerät zugreifen.
   - Drop (Ablehnen) – Diesen IP-Adressen wird der Zugriff auf das Dominion KX II-Gerät verweigert.



4. Klicken Sie auf "Append" (Anfügen). Die Regel wird unten in der Liste hinzugefügt. Wiederholen Sie die Schritte 1 bis 4, um weitere Regeln hinzuzufügen.

So fügen Sie eine Regel ein:

1. Geben Sie eine Regelnummer ein (#). Diese ist für den Befehl "Insert" (Einfügen) erforderlich.
2. Geben Sie Werte in die Felder "Starting IP" (IP-Startadresse) und "Ending IP" (IP-Endadresse) ein.
3. Wählen Sie in der Dropdownliste "Action" (Aktion) eine Option aus.
4. Klicken Sie auf "Insert" (Einfügen). Wenn die eingegebene Regelnummer einer bereits vorhandenen entspricht, wird die neue Regel vor der vorhandenen Regel eingefügt, und alle Regeln werden um eine Position nach unten verschoben.

So ersetzen Sie eine Regel:

1. Geben Sie die zu ersetzende Regelnummer an.
2. Geben Sie Werte in die Felder "Starting IP" (IP-Startadresse) und "Ending IP" (IP-Endadresse) ein.
3. Wählen Sie in der Dropdownliste "Action" (Aktion) eine Option aus.
4. Klicken Sie auf "Replace" (Ersetzen). Ihre neue Regel ersetzt die ursprüngliche Regel mit derselben Regelnummer.

So löschen Sie eine Regel:

1. Geben Sie die zu löschende Regelnummer an.
2. Klicken Sie auf "Delete" (Löschen).
3. Klicken Sie zum Bestätigen des Löschvorgangs auf OK.

Wichtig: ACL-Regeln werden in der Reihenfolge ausgewertet, in der sie aufgeführt sind. Werden die beiden ACL-Regeln in diesem Beispiel vertauscht, akzeptiert Dominion z. B. gar keine Kommunikation.

```
Rule 1, Starting IP = 192.168.50.1, Ending IP = 192.168.55.255, Action = ACCEPT

Rule 2, Starting IP = 0.0.0.0, Ending IP = 255.255.255.255, Action = DROP
```




Tipp: Mithilfe der Regelnummern können Sie die Reihenfolge, in der die Regeln erstellt werden, besser steuern.

Hinweis: Sowohl IPv4- als auch IPv6-Adressen werden unterstützt.

Ändern einer vorhandenen Benutzergruppe

Hinweis: Für die Gruppe "Admin" sind alle Berechtigungen aktiviert (dies kann nicht geändert werden).

So ändern Sie eine vorhandene Benutzergruppe:

1. Bearbeiten Sie auf der Seite "Group" (Gruppe) die entsprechenden Felder und legen Sie die gewünschten Berechtigungen fest.
2. Legen Sie unter "Permissions" (Berechtigungen) die Berechtigungen für die Gruppe fest. Aktivieren Sie die Kontrollkästchen für die Berechtigungen, die Sie allen Benutzern in dieser Gruppe gewähren möchten. Siehe Festlegen von Berechtigungen.
3. Legen Sie unter "Port Permissions" (Portberechtigungen) die Portberechtigungen fest. Legen Sie die für die Benutzer in dieser Gruppe zugänglichen Serverports fest, und geben Sie den Zugriffstyp an. Siehe **Festlegen von Portberechtigungen** (auf Seite 135).
4. Legen Sie die IP-ACL fest (optional). Mit diesem Feature beschränken Sie den Zugriff auf das Dominion KX II-Gerät, indem Sie IP-Adressen angeben. Siehe **Gruppenbasierte IP-ACL (IP-Zugriffssteuerungsliste)** (auf Seite 137).
5. Klicken Sie auf OK.

So löschen Sie eine Benutzergruppe:

Wichtig: Wenn Sie eine Gruppe mit Benutzern löschen, werden die Benutzer automatisch der Benutzergruppe <Unknown> (Unbekannt) zugewiesen.

Tipp: Um herauszufinden, welche Benutzer einer bestimmten Gruppe angehören, sortieren Sie die "User List" (Benutzerliste) nach "User Group" (Benutzergruppe).

1. Wählen Sie eine Gruppe aus der Liste aus, indem Sie das Kontrollkästchen links vom Gruppennamen aktivieren.
2. Klicken Sie auf "Delete" (Löschen).
3. Klicken Sie zum Bestätigen des Löschvorgangs auf OK.



Benutzer

Benutzern müssen Benutzernamen und Kennwörter zugeordnet werden, damit sie auf Dominion KX II zugreifen können. Anhand dieser Informationen werden Benutzer authentifiziert, die versuchen, auf Dominion KX II zuzugreifen. Für jede Benutzergruppe können bis zu 254 Benutzer erstellt werden.

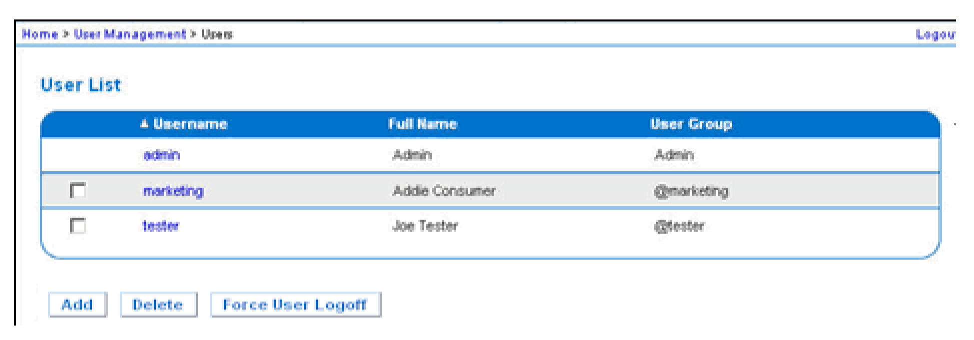
Wenn Sie eine Schichtkonfiguration verwenden, in der ein Dominion KX II-Basisgerät für den Zugriff auf mehrere andere Schichtgeräte verwendet wird, benötigen Benutzer die Zugriffsberechtigung für das Basisgerät sowie auf das individuelle Schichtgerät (bei Bedarf). Wenn sich Benutzer am Basisgerät anmelden, wird jedes Schichtgerät abgefragt und der Benutzer kann auf jeden Zielserver zugreifen, für den er Berechtigungen aufweist. Weitere Informationen zu Schichten finden Sie unter ***Konfigurieren und Aktivieren von Schichten*** (auf Seite 167).

User List (Benutzerliste)

Die Seite "User List" (Benutzerliste) enthält eine Liste aller Benutzer einschließlich des Benutzernamens, des vollständigen Namens und der Benutzergruppe. Klicken Sie auf einen Spaltennamen, um die Liste nach einer der Spalten zu sortieren. Auf der Seite "User List" (Benutzerliste) können Sie außerdem Benutzer hinzufügen, ändern oder löschen.

▶ So zeigen Sie die Benutzerliste an:

- Wählen Sie "User Management" > "User List" (Benutzerverwaltung > Benutzerliste) aus. Die Seite "User List" (Benutzerliste) wird angezeigt.





Hinzufügen eines neuen Benutzers

Es ist empfehlenswert, Benutzergruppen vor dem Erstellen von Dominion KX II-Benutzern zu definieren, da jeder Benutzer einer vorhandenen Benutzergruppe zugewiesen werden muss. Siehe **Hinzufügen einer neuen Benutzergruppe** (auf Seite 130).

Auf der Seite "User" (Benutzer) können Sie neue Benutzer hinzufügen, Benutzerinformationen ändern und deaktivierte Benutzer erneut aktivieren.

Hinweis: Ein Benutzername kann deaktiviert werden, wenn die Anzahl der fehlgeschlagenen Anmeldeversuche die auf der Seite "Security Settings" (Sicherheitseinstellungen) festgelegte maximale Anzahl der Anmeldeversuche überschritten hat. Siehe ***Sicherheitseinstellungen****.*

So fügen Sie einen neuen Benutzer hinzu:

1. Öffnen Sie die Seite "User" (Benutzer), indem Sie "User Management" > "Add New User Group" (Benutzerverwaltung > Neue Benutzergruppe hinzufügen) auswählen oder auf der Seite "User List" (Liste der Benutzer) auf die Schaltfläche "Add" (Hinzufügen) klicken.
2. Geben Sie im Feld "Username" (Benutzername) einen eindeutigen Namen ein (bis zu 16 Zeichen).
3. Geben Sie im Feld "Full Name" (Vollständiger Name) den vollständigen Namen des Benutzers ein (bis zu 64 Zeichen).
4. Geben Sie im Feld "Password" (Kennwort) ein Kennwort ein, und anschließend im Feld "Confirm Password" (Kennwort bestätigen) erneut (bis zu 64 Zeichen).
5. Wählen Sie in der Dropdownliste "User Group" (Benutzergruppe) die Gruppe aus. Die Liste enthält alle von Ihnen erstellten Gruppen sowie die vom System bereitgestellten Standardgruppen. <Unknown> (Unbekannt), welches die Standardeinstellung ist, "Admin" und "Individual Group" (Individuelle Gruppe).

   Wenn Sie diesen Benutzer keiner vorhandenen Benutzergruppe zuordnen möchten, wählen Sie in der Dropdownliste die Option "Individual Group" (Individuelle Gruppe) aus. Weitere Informationen zu den Berechtigungen einer individuellen Gruppe finden Sie unter ***Festlegen von Berechtigungen für eine individuelle Gruppe*** (auf Seite 136).
6. Aktivieren Sie das Kontrollkästchen "Active" (Aktiv), um den neuen Benutzer zu aktivieren. Standardmäßig ist dieses Kontrollkästchen aktiviert.
7. Klicken Sie auf OK.



Ändern eines vorhandenen Benutzers

So ändern Sie einen vorhandenen Benutzer:

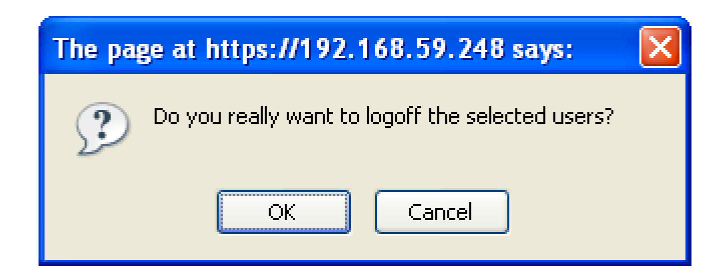
1. Öffnen Sie die Seite "User List" (Benutzerliste) unter "User Management" > "User List" (Benutzerverwaltung > Benutzerliste).
2. Wählen Sie den Benutzer aus der Liste auf der Seite "User List" (Benutzerliste) aus.
3. Klicken Sie auf den Benutzernamen. Die Seite "User" (Benutzer) wird angezeigt.
4. Bearbeiten Sie auf der Seite "User" (Benutzer) die entsprechenden Felder. Informationen zum Zugriff auf die Seite "User" (Benutzer) finden Sie unter ***Hinzufügen eines neuen Benutzers*** (auf Seite 141).
5. Klicken Sie auf "Delete" (Löschen), um einen Benutzer zu löschen. Sie werden aufgefordert, den Löschvorgang zu bestätigen.
6. Klicken Sie auf OK.

Abmelden eines Benutzers (Erzwungene Abmeldung)

Wenn Sie Administrator sind, können Sie andere lokal authentifizierte Benutzer, die an Dominion KX II angemeldet sind, abmelden.

So melden Sie einen Benutzer ab:

1. Öffnen Sie die Seite "User List" (Benutzerliste) unter "User Management" > "User List" (Benutzerverwaltung > Benutzerliste) oder klicken Sie auf den Link "Connected User" (Verbundene Benutzer) auf der linken Bildschirmseite.
2. Wählen Sie den Benutzer aus der Liste auf der Seite "User List" (Benutzerliste) aus und aktivieren Sie das Kontrollkästchen neben dem jeweiligen Benutzernamen.
3. Klicken Sie auf die Schaltfläche "Force User Logoff" (Erzwungene Benutzerabmeldung).
4. Klicken Sie im Dialogfeld "Logoff User" (Benutzer abmelden) auf OK, um den Benutzer abzumelden.





5. Eine Bestätigungsmeldung über die erfolgreiche Benutzerabmeldung wird angezeigt. Diese Meldung enthält das Datum und die Uhrzeit der Abmeldung. Klicken Sie zum Schließen der Meldung auf OK.

Authentication Settings (Authentifizierungseinstellungen)

Bei der Authentifizierung geht es darum, die Identität des Benutzers zu überprüfen. Nach der Authentifizierung dient die Benutzergruppe dazu, die jeweiligen System- und Port-Berechtigungen zu ermitteln. Die dem Benutzer zugewiesenen Berechtigungen legen fest, welche Art des Zugriffs zulässig ist. Dies nennt man Autorisierung.

Wenn Dominion KX II zur Remote-Authentifizierung konfiguriert ist, wird der externe Authentifizierungsserver hauptsächlich zur Authentifizierung verwendet und nicht zur Autorisierung.

Wenn Sie eine Schichtkonfiguration verwenden, in der ein Dominion KX II-Basisgerät für den Zugriff auf mehrere andere Schichtgeräte verwendet wird, müssen das Basisgerät und die Schichtgeräte dieselben Authentifizierungseinstellungen verwenden.

Auf der Seite "Authentication Settings" (Authentifizierungseinstellungen) können Sie die Art der Authentifizierung für den Zugriff auf Dominion KX II konfigurieren.

Hinweis: Wird der Benutzer bei aktivierter Remoteauthentifizierung (LDAP/LDAPS oder RADIUS) nicht gefunden, wird zusätzlich die Authentifizierungsdatenbank geprüft.

So konfigurieren Sie die Authentifizierung:

1. Wählen Sie "User Management" > "Authentication Settings" (Benutzerverwaltung > Authentifizierungseinstellungen) aus. Die Seite "Authentication Settings" (Authentifizierungseinstellungen) wird angezeigt.
2. Wählen Sie die Option für das gewünschte Authentifizierungsprotokoll aus. Zur Verfügung stehen "Local Authentication" (Lokale Authentifizierung), "LDAP/LDAPS" oder "RADIUS". Bei Auswahl der Option "LDAP" werden die restlichen LDAP-Felder aktiviert, bei Auswahl der Option "RADIUS" die restlichen RADIUS-Felder.
3. Wenn Sie "Local Authentication" (Lokale Authentifizierung) auswählen, fahren Sie mit Schritt 6 fort.
4. Wenn Sie sich für "LDAP/LDAPS" entscheiden, lesen Sie den Abschnitt Implementierung der LDAP-Remoteauthentifizierung. Dort finden Sie Informationen zum Ausfüllen der Felder im Abschnitt "LDAP" der Seite "Authentication Settings" (Authentifizierungseinstellungen).

5. Wenn Sie sich für "RADIUS" entscheiden, lesen Sie den Abschnitt Implementierung der RADIUS-Remoteauthentifizierung. Dort finden Sie Informationen zum Ausfüllen der Felder im Abschnitt "RADIUS" der Seite "Authentication Settings" (Authentifizierungseinstellungen).
6. Klicken Sie zum Speichern auf OK.

So kehren Sie zu den Werkseinstellungen zurück:

- Klicken Sie auf die Schaltfläche "Reset to Defaults" (Auf Standardeinstellungen zurücksetzen).

Implementierung der LDAP/LDAPS-Remoteauthentifizierung

Lightweight Directory Access Protocol (LDAP/LDAPS) ist ein Netzwerkprotokoll für die Abfrage und Änderung von Verzeichnisdiensten, die über TCP/IP ausgeführt werden. Ein Client startet eine LDAP-Sitzung, indem er eine Verbindung mit einem LDAP/LDAPS-Server herstellt (Standard-TCP-Port: 389). Anschließend sendet der Client Anfragen an den Server, und der Server sendet Antworten zurück.

Erinnerung: Microsoft Active Directory fungiert als LDAP/LDAPS-Authentifizierungsserver.

So verwenden Sie das LDAP-Authentifizierungsprotokoll:

1. Klicken Sie auf "User Management" > "Authentication Settings" (Benutzerverwaltung > Authentifizierungseinstellungen), um die Seite "Authentication Settings" (Authentifizierungseinstellungen) zu öffnen.
2. Wählen Sie das Optionsfeld "LDAP" aus, um den Abschnitt "LDAP" der Seite zu aktivieren.
3. Klicken Sie auf das LDAP-Symbol, um den Abschnitt "LDAP" zu erweitern.

Serverkonfiguration

4. Geben Sie im Feld "Primary LDAP Server" (Primärer LDAP-Server) die IP-Adresse oder den DNS-Namen des LDAP/LDAPS-Remote-Authentifizierungsservers ein (bis zu 256 Zeichen). Sind die Optionen "Enable Secure LDAP" (Secure LDAP aktivieren) und "Enable LDAPS Server Certificate Validation" (LDAPS-Serverzertifikat-Validierung aktivieren) ausgewählt, muss der DNS-Name verwendet werden, um dem CN des LDAP-Serverzertifikats zu entsprechen.



5. Geben Sie im Feld "Secondary LDAP Server" (Sekundärer LDAP-Server) die IP-Adresse oder den DNS-Namen des LDAP/LDAPS-Sicherungsservers ein (bis zu 256 Zeichen). Wenn die Option "Enable Secure LDAP" (Secure LDAP aktivieren) ausgewählt ist, muss der DNS-Name verwendet werden. Für die restlichen Felder gelten die gleichen Einstellungen wie für "Primary LDAP Server" (Primärer LDAP-Server). **Optional**
6. "Type of external LDAP Server" (Typ des externen LDAP-Servers)
7. Geben Sie den Namen der Active Directory-Domäne ein, Zum Beispiel *testradius.com*. Fragen Sie Ihren leitenden Administrator nach einem speziellen Dömanennamen.
8. Geben Sie in das Feld "User Search DN" (DN für Benutzersuche) den Distinguished Name ein, bei dem Sie die Suche nach Benutzerinformationen in der LDAP-Datenbank beginnen möchten. Es können bis zu 64 Zeichen verwendet werden. Ein Beispiel für einen Basissuchwert ist: `cn=Benutzer,dc=raritan,dc=com`. Fragen Sie den Administrator des Authentifizierungsservers nach den korrekten Werten für diese Felder.
9. Geben Sie den Distinguished Name (DN) des Administratorbenutzers in das Feld "DN of Administrative User" (DN des Administratorbenutzers) ein (maximal 64 Zeichen). Füllen Sie dieses Feld aus, wenn Ihr LDAP-Server nur Administratoren die Suche nach Benutzerinformationen mithilfe der Funktion "Administrative User" (Administratorbenutzer) gestattet. Fragen Sie den Administrator des Authentifizierungsservers nach den korrekten Werten für dieses Feld. Ein Wert für "DN of administrative User" (DN des Administratorbenutzers) könnte wie folgt aussehen: `cn=Administrator,cn=Benutzer,dc=testradius,dc=com`. **Optional**

10. Wenn Sie einen "Distinguished Name" (DN) für den Administratorbenutzer eingeben, müssen Sie das Kennwort eingeben, um den DN des Administratorbenutzers am Remote-Authentifizierungsserver zu authentifizieren. Geben Sie das Kennwort in das Feld "Secret Phrase" (Geheimer Schlüssel) und ein weiteres Mal in das Feld "Confirm Secret Phrase" (Geheimen Schlüssel bestätigen) ein (maximal 128 Zeichen).

Authentication Settings

Local Authentication
LDAP
RADIUS

▼ LDAP

Server Configuration

Primary LDAP Server
192.168.59.187
Secondary LDAP Server (optional)
192.168.51.214
Type of External LDAP Server
Microsoft Active Directory
Active Directory Domain
testradius.com
User Search DN
cn=users,dc=testradius,dc=com
DN of Administrative User (optional)
cn=Administrator,cn=users,dc=testrac
Secret Phrase of Administrative User
••••••••
Confirm Secret Phrase

LDAP/Secure LDAP

11. Aktivieren Sie das Kontrollkästchen "Enable Secure LDA" (Secure LDAP aktivieren), wenn Sie SSL verwenden möchten. Dadurch wird das Kontrollkästchen "Enable LDAPS Server Certificate Validation" (LDAPS-Serverzertifikat-Validierung aktivieren) aktiviert. Secure Sockets Layer (SSL) ist ein kryptografisches Protokoll, über das Dominion KX II sicher mit dem LDAP/LDAPS-Server kommunizieren kann.



12. Der Standardport lautet 389. Verwenden Sie entweder den Standard-TCP-Port für LDAP oder legen Sie einen anderen Port fest.
13. Der standardmäßige Secure LDAP-Port lautet 636. Verwenden Sie entweder den Standardport oder legen Sie einen anderen Port fest. Dieses Feld wird nur verwendet, wenn das Kontrollkästchen "Enable Secure LDAP" (Secure LDAP aktivieren) aktiviert ist.
14. Aktivieren Sie das Kontrollkästchen "Enable LDAPS Server Certificate Validation" (LDAPS-Serverzertifikat-Validierung aktivieren), und verwenden Sie die zuvor hochgeladene CA-Stammzertifikatdatei zur Validierung des vom Server bereitgestellten Zertifikats. Wenn Sie die zuvor hochgeladene CA-Stammzertifikatdatei nicht verwenden möchten, lassen Sie das Kontrollkästchen deaktiviert. Die Deaktivierung dieser Funktion entspricht der Annahme des Zertifikats einer unbekannten Zertifizierungsstelle. Dieses Kontrollkästchen ist nur verfügbar, wenn das Kontrollkästchen "Enable Secure LDAP" (Secure LDAP aktivieren) aktiviert wurde.

Hinweis: Ist zusätzlich zur CA-Stammzertifikat-Validierung die Option "Enable LDAPS Server Certificate Validation" (LDAPS-Serverzertifikat-Validierung aktivieren) aktiviert, muss der Hostname des Servers mit dem bereitgestellten allgemeinen Namen im Serverzertifikat übereinstimmen.



15. Laden Sie die CA-Stammzertifikatdatei hoch, falls dies erforderlich ist. Dieses Feld steht zur Verfügung, wenn das Kontrollkästchen "Enable Secure LDAP" (Secure LDAP aktivieren) aktiviert ist. Fragen Sie den Administrator des Authentifizierungsservers nach der CA-Zertifikatdatei im Base64-codierten X-509-Format für den LDAP-/LDAPS-Server. Navigieren Sie über die Schaltfläche "Browse" (Durchsuchen) zur entsprechenden Zertifikatdatei. Wenn Sie ein Zertifikat für den LDAP-/LDAPS-Server durch ein neues Zertifikat ersetzen, müssen Sie Dominion KX II neu starten, damit das neue Zertifikat wirksam wird.



Testen des LDAP-Serverzugriffs

16. Dominion KX II bietet Ihnen aufgrund der Komplexität einer erfolgreichen Konfigurierung von LDAP-Server und Dominion KX II zur Remoteauthentifizierung die Möglichkeit, die LDAP-Konfigurierung auf der Seite "Authentication Settings" (Authentifizierungseinstellungen) zu testen. Um die Authentifizierungseinstellungen zu testen, geben Sie den Anmeldenamen in das das Feld "Login for testing" (Anmeldung für Test) und das Kennwort in das Feld "Password for testing" (Kennwort für Test) ein. Das sind der Benutzername und das Kennwort, die Sie für den Zugriff auf Dominion KX II eingegeben haben und die vom LDAP-Server für Ihre Authentifizierung verwendet werden. Klicken Sie auf "Test".



Ist der Test abgeschlossen, wird Ihnen in einer Meldung angezeigt, ob der Test erfolgreich war oder nicht. Ist der Test fehlgeschlagen, wird Ihnen eine detaillierte Fehlermeldung angezeigt. Es wird das Ergebnis des erfolgreich durchgeführten Tests oder, falls der Test nicht erfolgreich war, eine detaillierte Fehlermeldung angezeigt. Außerdem können Gruppeninformationen angezeigt werden, die im Falle eines erfolgreichen Tests für den Testbenutzer vom LDAP-Remoteserver abgerufen werden.

Test LDAP Server Access

Login for testing

Password for testing

Test

Rückgabe von Benutzergruppeninformationen vom Active Directory-Server

Dominion KX II unterstützt die Benutzerauthentifizierung zu Active Directory® (AD), ohne dass Benutzer lokal in Dominion KX II definiert sein müssen. Dadurch können Active Directory-Benutzerkonten und -Kennwörter ausschließlich auf dem Active Directory-Server verwaltet werden. Die Autorisierungs- und Active Directory-Benutzerrechte werden mit standardmäßigen Dominion KX II-Richtlinien und Benutzergruppenrechten, die lokal auf Active Directory-Benutzergruppen angewendet werden, gesteuert und verwaltet.

WICHTIG: Wenn Sie bereits Kunde von Raritan, Inc. sind und den Active Directory-Server bereits durch Ändern des Active Directory-Schemas konfiguriert haben, unterstützt Dominion KX II diese Konfiguration nach wie vor, und Sie müssen den folgenden Vorgang nicht durchführen. Informationen zur Aktualisierung des Active Directory-LDAP/LDAPS-Schemas finden Sie unter Aktualisieren des LDAP-Schemas.

▸ So aktivieren Sie den Active Directory-Server auf der Dominion KX II-Einheit:

1. Erstellen Sie auf der Dominion KX II-Einheit besondere Gruppen und weisen Sie ihnen geeignete Berechtigungen zu. Erstellen Sie z. B. Gruppen wie "KVM_Admin" und "KVM_Operator".
2. Erstellen Sie auf dem Active Directory-Server neue Gruppen mit denselben Gruppennamen wie die im vorherigen Schritt erstellten Gruppen.



3. Weisen Sie die Dominion KX II-Benutzer auf dem AD-Server den Gruppen zu, die Sie in Schritt 2 erstellt haben.
4. Aktivieren und konfigurieren Sie den AD-Server auf der Dominion KX II-Einheit ordnungsgemäß. Siehe Implementierung der LDAP/LDAPS-Remoteauthentifizierung.

Wichtige Hinweise:

- Bei der Eingabe des Gruppennamens muss die Groß-/Kleinschreibung beachtet werden.
- Dominion KX II bietet folgende Standardgruppen, die nicht geändert oder gelöscht werden können: Admin und <Unknown> (Unbekannt). Stellen Sie sicher, dass diese Gruppennamen nicht auch vom Active Directory-Server verwendet werden.
- Wenn die vom Active Directory-Server zurückgegebenen Gruppeninformationen nicht mit einer Dominion KX II-Gruppenkonfiguration übereinstimmen, weist Dominion KX II den Benutzern, die sich erfolgreich authentifizieren, automatisch die Gruppe <Unknown> (Unbekannt) zu.
- Wenn Sie eine Rückrufnummer verwenden, müssen Sie die folgende Zeichenfolge unter Beachtung der Groß-/Kleinschreibung eingeben: *msRADIUSCallbackNumber.*
- Auf Empfehlung von Microsoft sollten "Global Groups" (globale Gruppen) mit Benutzerkonten verwendet werden, keine "Domain Local Groups" (lokale Domaingruppen).

Implementierung der RADIUS-Remoteauthentifizierung

Remote Authentication Dial-in User Service (RADIUS) ist ein AAA-Protokoll [Authentication, Authorization Accounting (Authentifizierung, Autorisierung und Kontoführung)] für Anwendungen für den Netzwerkzugriff.

► So verwenden Sie das RADIUS-Authentifizierungsprotokoll:

1. Klicken Sie auf "User Management" > "Authentication Settings" (Benutzerverwaltung > Authentifizierungseinstellungen), um die Seite "Authentication Settings" (Authentifizierungseinstellungen) zu öffnen.
2. Klicken Sie auf das Optionsfeld "RADIUS", um den Abschnitt "RADIUS" der Seite zu aktivieren.
3. Klicken Sie auf das ► RADIUS-Symbol, um den Abschnitt "RADIUS" zu erweitern.



4. Geben Sie in den Feldern "Primary Radius Server" (Primärer RADIUS-Server) und "Secondary Radius Server" (Sekundärer RADIUS-Server) die jeweiligen IP-Adressen des primären und optionalen sekundären Remote-Authentifizierungsservers ein (bis zu 256 Zeichen).
5. Geben Sie im Feld "Shared Secret" (Gemeinsamer geheimer Schlüssel) den geheimen Schlüssel für die Authentifizierung ein (bis zu 128 Zeichen).

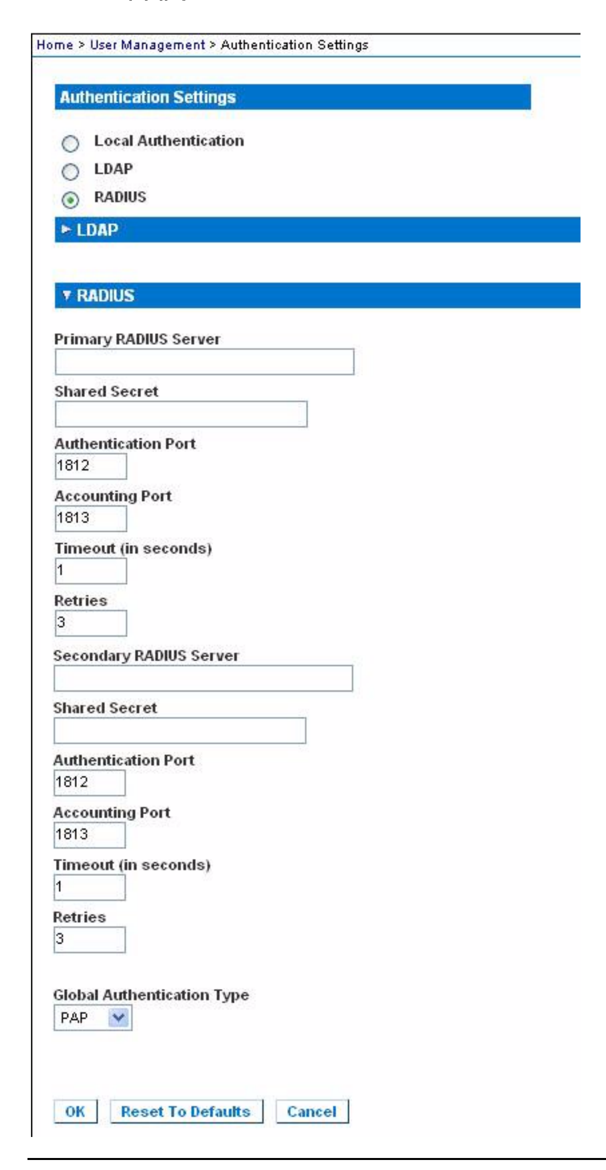
   Der gemeinsame geheime Schlüssel ist eine Zeichenfolge, die Dominion KX II und dem RADIUS-Server bekannt sein muss, damit diese sicher kommunizieren können. Es handelt sich dabei praktisch um ein Kennwort.
6. Der Standardport für "Authentication Port" (Authentifizierungsport) lautet 1812, kann jedoch nach Bedarf geändert werden.
7. Der Standardport für "Accounting Port" (Kontoführungsport) lautet 1813, kann jedoch nach Bedarf geändert werden.
8. Das "Timeout" (Zeitlimit) wird in Sekunden aufgezeichnet. Der Standardwert beträgt 1 Sekunde, kann jedoch bei Bedarf geändert werden.

   Das Zeitlimit bezeichnet die Zeitspanne, während der Dominion KX II auf eine Antwort vom RADIUS-Server wartet, ehe eine weitere Authentifizierungsanforderung gesendet wird.
9. Die standardmäßige Anzahl an Neuversuchen beträgt 3.

   Dieser Wert gibt an, wie oft Dominion KX II eine Authentifizierungsanforderung an den RADIUS-Server sendet.
10. Wählen Sie in der Dropdownliste den "Global Authentication Type" (Globaler Authentfizierungstyp) aus:

    - PAP – Mit PAP werden Kennwörter als unformatierter Text gesendet. PAP ist nicht interaktiv. Benutzername und Kennwort werden als ein Datenpaket gesendet, sobald eine Verbindung hergestellt wurde. Der Server sendet nicht zuerst eine Anmeldeaufforderung und wartet auf eine Antwort.

- CHAP – Mit CHAP kann der Server jederzeit eine Authentifizierung anfordern. CHAP bietet mehr Sicherheit als PAP.



Hinweis: Sowohl IPv4- als auch IPv6-Adressen werden unterstützt.



Zurückgeben von Benutzergruppeninformationen über RADIUS

Wenn ein RADIUS-Authentifizierungsversuch erfolgreich ist, bestimmt Dominion KX II die Berechtigungen eines Benutzers anhand der Berechtigungen der Gruppe des Benutzers.

Ihr Remote-RADIUS-Server kann diese Benutzergruppennamen bereitstellen, indem er ein als RADIUS FILTER-ID implementiertes Attribut zurückgibt. Die FILTER-ID sollte folgendermaßen formatiert sein: Raritan:G{*GROUP_NAME*}. Dabei ist *GROUP_NAME* eine Zeichenfolge, die den Namen der Gruppe angibt, der der Benutzer angehört.

Raritan:G{GROUP_NAME}:D{Dial Back Number}

Dabei ist "GROUP_NAME" eine Zeichenfolge, die den Namen der Gruppe angibt, der der Benutzer angehört, und "Dial Back Number" die dem Benutzerkonto zugeordnete Nummer, die das Dominion KX II-Modem für den Rückruf des Benutzerkontos verwendet.

Spezifikationen für den RADIUS-Kommunikationsaustausch

Dominion KX II sendet die folgenden RADIUS-Attribute an Ihren RADIUS-Server:

Attribut	Daten
Anmelden	
Access-Request (1)	
NAS-Port-Type (61)	VIRTUAL (5) für Netzwerkverbindungen.
NAS-IP-Address (4)	Die IP-Adresse des Dominion KX II.
User-Name (1)	Dies ist der in der Anmeldemaske eingegebene Benutzername.
Acct-Session-ID (44)	Sitzungs-ID für Kontoführung.
User-Password(2)	Das verschlüsselte Kennwort.
Accounting-Request(4)	
Acct-Status (40)	Start(1) – Kontoführung wird gestartet.
NAS-Port-Type (61)	VIRTUAL (5) für Netzwerkverbindungen.
NAS-Port (5)	Dieses Attribut ist immer 0.
NAS-IP-Address (4)	Die IP-Adresse des Dominion KX II.
User-Name (1)	Dies ist der in der Anmeldemaske eingegebene Benutzername.
Acct-Session-ID (44)	Sitzungs-ID für Kontoführung.

Attribut Anmelden Abmelden	Daten
Accounting-Request(4)	
Acct-Status (40)	Stop(2) – Kontoführung wird beendet.
NAS-Port-Type (61)	VIRTUAL (5) für Netzwerkverbindungen.
NAS-Port (5)	Dieses Attribut ist immer 0.
NAS-IP-Address (4)	Die IP-Adresse des Dominion KX II.
User-Name (1)	Dies ist der in der Anmeldemaske eingegebene Benutzername.
Acct-Session-ID (44)	Sitzungs-ID für Kontoführung.



Benutzerauthentifizierungsprozess

Die Remoteauthentifizierung wird über den im folgenden Diagramm angegebenen Vorgang durchgeführt:

User logs in

Is Remote Authentication Enabled ?

No

Yes

Is Remote Authentication Server reachable ?

No

No

Yes

Is User authenticated in local database ?

Is User authenticated in remote database ?

Yes

Yes

User allowed

No

User denied

Ändern von Kennwörtern

So ändern Sie Ihr Kennwort:

1. Wählen Sie "User Management" > "Change Password" (Benutzerverwaltung > Kennwort ändern). Die Seite "Change Password" (Kennwort ändern) wird angezeigt.
2. Geben Sie im Feld "Old Password" (Altes Kennwort) Ihr aktuelles Kennwort ein.
3. Geben Sie in das Feld "New Password" (Neues Kennwort) ein neues Kennwort ein. Geben Sie das Kennwort im Feld "Confirm New Password" (Neues Kennwort bestätigen) erneut ein. Ein Kennwort kann aus bis zu 64 alphanumerischen Zeichen der englischen Sprache sowie Sonderzeichen bestehen.
4. Klicken Sie auf OK.
5. Die erfolgreiche Änderung des Kennworts wird bestätigt. Klicken Sie auf OK.

Hinweis: Wenn sichere Kennwörter verwendet werden müssen, enthält diese Seite Informationen zum erforderlichen Format. Weitere Informationen zu Kennwörtern und sicheren Kennwörtern finden Sie unter **Sichere Kennwörter** *(siehe "***Strong Passwords (Sichere Kennwörter)***" auf Seite 234).*

Home > User Management > Change Password

Change Password

Old Password

New Password

Confirm New Password

OK Cancel



Kapitel 8 Geräteverwaltung

In diesem Kapitel

Netzwerkeinstellungen

Auf der Seite "Network Settings" (Netzwerkeinstellungen) können Sie die Netzwerkkonfiguration (z. B. IP-Adresse, Erkennungsport und LAN-Schnittstellenparameter) für Ihre Dominion KX II-Einheit anpassen.

Es stehen Ihnen zwei Optionen zum Festlegen der IP-Konfiguration zur Verfügung:

- None (default) [Keine (Standard)] – Dies ist die empfohlene Option (statisches IP). Da die Dominion KX II-Einheit Teil Ihrer Netzwerkinfrastruktur ist, möchten Sie wahrscheinlich, dass die Adresse möglichst konstant bleibt. Bei dieser Option können Sie die Netzwerkparameter selbst einrichten.
- DHCP – Mit dieser Option wird die IP-Adresse automatisch durch einen DHCP-Server zugewiesen.

So ändern Sie die Netzwerkkonfiguration:

1. Wählen Sie "Device Settings" > "Network" (Geräteeinstellungen > Netzwerk) aus. Die Seite "Network Settings" (Netzwerkeinstellungen) wird angezeigt.
2. Aktualisieren der Basisnetzwerkeinstellungen. Siehe Basisnetzwerkeinstellungen.
3. Aktualisieren der LAN-Schnittstelleneinstellungen. Siehe LAN-Schnittstelleneinstellungen.
4. Klicken Sie auf OK, um die Konfiguration festzulegen. Ist für die vorgenommenen Änderungen ein Neustart des Geräts erforderlich, wird eine entsprechende Meldung angezeigt.

So kehren Sie zu den Werkseinstellungen zurück:

- Klicken Sie auf "Reset to Defaults" (Standardeinstellungen wiederherstellen).

Hinweis: Sowohl IPv4- als auch IPv6-Adressen werden unterstützt.

Basisnetzwerkeinstellungen

Im Folgenden wird das Zuweisen einer IP-Adresse auf der Seite "Network Settings" (Netzwerkeinstellungen) beschrieben. Umfassende Informationen zu allen Feldern sowie zur Funktionsweise dieser Seite finden Sie unter ***Netzwerkeinstellungen*** (auf Seite 157).

1. Wählen Sie "Device Settings" > "Network" (Geräteeinstellungen > Netzwerk) aus. Die Seite "Network Settings" (Netzwerkeinstellungen) wird angezeigt.
2. Geben Sie einen aussagekräftigen Namen für Ihr Dominion KX II-Gerät an. Verwenden Sie dazu bis zu 32 gültige Sonderzeichen und keine Leerzeichen.
3. Geben Sie im Bereich "IPv4" die entsprechenden IPv4-spezifischen Netzwerkeinstellungen ein oder wählen Sie diese aus:
   a. Geben Sie eine IP-Adresse ein, falls erforderlich. Die Standard-IP-Adresse lautet 192.168.0.192.
   b. Geben Sie die Subnetzmaske ein. Die Standardsubnetzmaske lautet 255.255.255.0.
   c. Geben Sie das Standardgateway ein, wenn in der Dropdownliste unter "IP Auto Configuration" (Automatische IP-Konfiguration) "None" (Keine) ausgewählt ist.
   d. Geben Sie den Namen des bevorzugten DHCP-Hosts ein, wenn in der Dropdownliste unter "IP Auto Configuration" (Automatische IP-Konfiguration) "DHCP" ausgewählt ist.
   e. Wählen Sie "IP Auto Configuration" (Automatische IP-Konfiguration) aus. Folgende Optionen stehen zur Verfügung:
   - None (Static IP) [Keine (Statisches IP)] – Bei Auswahl dieser Option müssen Sie die Netzwerkparameter manuell angeben.

     Diese Option wird empfohlen, da Dominion KX II ein Infrastrukturgerät ist, dessen IP-Adresse sich nicht ändern sollte.
   - DHCP – Dynamic Host Configuration Protocol wird von Netzwerkcomputern (Clients) verwendet, um eindeutige IP-Adressen und andere Parameter von einem DHCP-Server zu erhalten.



Bei Auswahl dieser Option gibt der DHCP-Server die Netzwerkparameter an. Bei Verwendung von DHCP geben Sie den Namen des bevorzugten Hosts ein (nur DHCP) (maximal 63 Zeichen).

4. Wenn IPv6 verwendet werden soll, geben Sie im Bereich "IPv6" die entsprechenden IPv6-spezifischen Netzwerkeinstellungen ein oder wählen Sie diese aus:

   a. Aktivieren Sie das Kontrollkästchen "IPv6", um die Felder in diesem Bereich zu aktivieren.

   b. Geben Sie eine globale/eindeutige IP-Adresse ein. Dies ist die IP-Adresse, die dem Dominion KX II zugeordnet ist.

   c. Geben Sie die Präfixlänge ein. Dies ist die Anzahl der Bits, die in der IPv6-Adresse verwendet werden.

   d. Geben Sie die IP-Adresse des Gateway ein.

   e. Link-Local-IP-Adresse. Diese Adresse wird dem Gerät automatisch zugewiesen. Sie wird zum Erkennen von Nachbarn verwendet oder wenn keine Router verfügbar sind. **Read-Only (Lesezugriff)**

   f. Zonen-ID. Hierdurch wird das Gerät identifiziert, dem die Adresse zugeordnet ist. **Read-Only (Lesezugriff)**

   g. Wählen Sie "IP Auto Configuration" (Automatische IP-Konfiguration) aus. Folgende Optionen stehen zur Verfügung:

   - None (Keine) – Wählen Sie diese Option aus, wenn Sie keine automatische IP-Konfiguration wünschen, sondern die IP-Adresse lieber selbst festlegen (statisches IP). Diese Option ist voreingestellt und wird empfohlen.

     Wenn für "IP auto configuration" (Automatische IP-Konfiguration) "None" (Keine) ausgewählt ist, sind die folgenden "Network Basic Settings" (Basisnetzwerkeinstellungen) aktiviert: "Global/Unique IP Address" (Globale/Eindeutige IP-Adresse), "Prefix Length" (Präfixlange) und "Gateway IP Address" (Gateway-IP-Adresse) ermöglichen Ihnen die manuelle IP-Konfiguration.

   - Router Discovery (Router-Erkennung) – Verwenden Sie diese Option, um IPv6-Adressen, deren Signifikanz "Global" oder "Unique Local" (Lokal eindeutig) ist und über der von Link Local liegt, welche nur für ein direkt verbundenes Subnetz gültig ist, automatisch zuzuordnen.

5. Wenn DHCP ausgewählt ist, wählen Sie "Obtain DNS Server Address Automatically" (DNS-Serveradresse automatisch abrufen) aus, um diese Funktion zu aktivieren. Wenn die DNS-Serveradresse automatisch abgerufen wird, werden die vom DHCP-Server bereitgestellten DNS-Informationen verwendet.

6. Wenn "Use the Following DNS Server Addresses" (Die folgenden DNS-Serveradressen verwenden) ausgewählt ist, werden die in diesem Abschnitt eingegebenen Adressen für die Verbindung zum DNS-Server verwendet, unabhängig davon, ob DHCP ausgewählt wurde.

   Geben Sie die folgenden Informationen ein, wenn die Option "Following DNS Server Addresses" (Folgende DNS-Serveradressen) ausgewählt wurde. Diese Adressen sind die primären und sekundären DNS-Adressen, die verwendet werden, wenn die primäre DNS-Serververbindung aufgrund eines Ausfalls getrennt wird.

   a. Primary DNS Server IP Address (IP-Adresse des primären DNS-Servers)

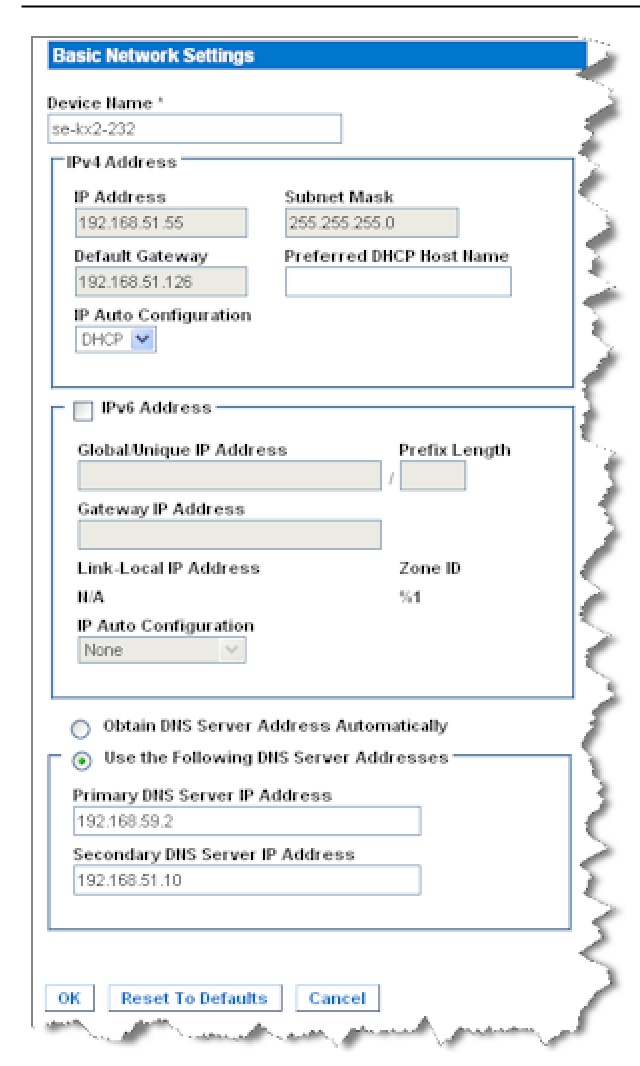
   b. Secondary DNS-Server IP Address (IP-Adresse des sekundären DNS-Servers)

7. Klicken Sie abschließend auf OK. Das Dominion KX II-Gerät ist jetzt über das Netzwerk zugänglich.



Weitere Informationen zur Konfiguration dieses Bereichs der Seite "Network Settings" (Netzwerkeinstellungen) finden Sie unter ***LAN-Schnittstelleneinstellungen*** (auf Seite 162).

Hinweis: Bei manchen Umgebungen gibt die Standardeinstellung "Autodetect" (automatische Aushandlung) für "LAN Interface Speed & Duplex" (LAN-Schnittstellengeschwindigkeit und Duplex) die Netzwerkparameter nicht richtig vor, was zu Netzwerkproblemen führen kann. Wählen Sie in einem solchen Fall im Feld "LAN Interface Speed & Duplex" des Dominion KX II den Wert "100 Mbps/Full Duplex" (100 Mbit/s/Vollduplex) (bzw. die geeignete Option für Ihr Netzwerk) aus, um dieses Problem zu beheben. Weitere Informationen finden Sie auf der Seite **Network Settings** *(siehe "***Netzwerkeinstellungen***" auf Seite 157) (Netzwerkeinstellungen).*



LAN-Schnittstelleneinstellungen

1. Die aktuellen Parametereinstellungen werden im Feld "Current LAN Interface Parameters" (Aktuelle LAN-Schnittstellenparameter) angezeigt.
2. Wählen Sie aus folgenden Optionen die LAN-Schnittstellengeschwindigkeit & Duplex aus:
   - Autodetect [automatische Aushandlung (Standardoption)]
   - 10 Mbit/s/Halb – Beide LEDs blinken
   - 10 Mbit/s/Voll – Beide LEDs blinken
   - 100 Mbit/s/Halb – Gelbe LED blinkt
   - 100 Mbit/s/Voll – Gelbe LED blinkt
   - 1000 Mbit/s/Voll (Gigabit) – grüne LED blinkt
   - "Half-duplex" (Halbduplex) sorgt für Kommunikation in beide Richtungen, jedoch nicht gleichzeitig.
   - "Full-duplex" (Vollduplex) ermöglicht die gleichzeitige Kommunikation in beide Richtungen.

   Hinweis: Bei 10 Mbit/s und Halb- oder Vollduplex kann es gelegentlich zu Problemen kommen. Verwenden Sie in einem solchen Fall eine andere Geschwindigkeit und Duplexeinstellung.

   Weitere Informationen finden Sie unter ***Netzwerk-Geschwindigkeitseinstellungen*** (auf Seite 331).
3. Aktivieren Sie das Kontrollkästchen "Enable Automatic Failover" (Automatisches Failover aktivieren), um zu veranlassen, dass Dominion KX II die Netzwerkverbindung automatisch mithilfe eines zweiten Netzwerkports wiederherstellt, wenn der aktive Netzwerkport ausfällt.

   Hinweis: Da ein Failoverport erst aktiviert wird, wenn tatsächlich ein Ausfall stattgefunden hat, empfiehlt Raritan, den Port nicht zu überwachen oder ihn erst zu überwachen, nachdem ein Ausfall stattgefunden hat.

   Wenn dieses Kontrollkästchen aktiviert ist, stehen die folgenden beiden Felder zur Verfügung:
   - Ping Interval (seconds) (Pingintervall [Sekunden]) – Mit dem Pingintervall wird festgelegt, wie häufig Dominion KX II den Status des Netzwerkpfads zum festgelegten Gateway prüft. Das Standardpingintervall beträgt 30 Sekunden.
   - Timeout (seconds) (Zeitlimit [Sekunden]) – Das Zeitlimit bestimmt, wie lange ein festgelegtes Gateway über die Netzwerkverbindung nicht erreichbar sein darf, bevor ein Fehler auftritt.



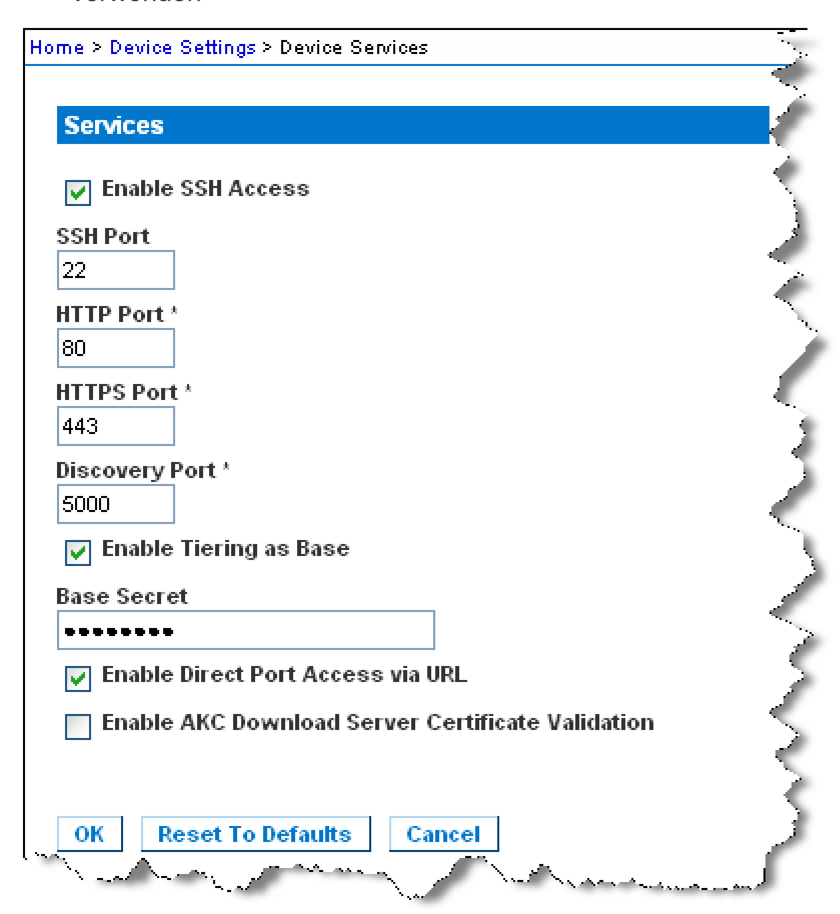
Hinweis: Pingintervall und Zeitlimit können durch Konfiguration optimal an die Bedingungen des Netzwerks angepasst werden. Die Einstellung für das Zeitlimit sollte so gewählt werden, dass mindestens 2 oder mehr Pinganforderungen übertragen und beantwortet werden können. Wird beispielsweise eine hohe Failover-Rate aufgrund von starker Netzwerkauslastung beobachtet, sollte das Zeitlimit auf das 3- bis 4-fache des Pingintervalls erhöht werden.

4. Wählen Sie aus den folgenden Optionen die Bandbreite aus:
   - 100 Megabit
   - 10 Megabit
   - 5 Megabit
   - 2 Megabit
   - 512 Kilobit
   - 256 Kilobit
   - 128 Kilobit
5. Klicken Sie auf OK, um die LAN-Einstellungen zu übernehmen.

Device Services (Gerätedienste)

Auf der Seite "Device Services" (Gerätedienste) können Sie die folgenden Funktionen konfigurieren:

- SSH-Zugriff aktivieren
- Schichten für das Basis-Dominion KX II aktivieren
- Erkennungsport eingeben
- Direkten Portzugriff aktivieren
- AKC-Download-Serverzertifikat-Validierung aktivieren, falls Sie AKC verwenden





Aktivieren von SSH

Wählen Sie "Enable SSH Access" (SSH-Zugriff aktivieren) aus, damit Administratoren über die SSH v2-Anwendung auf Dominion KX II zugreifen können.

So aktivieren Sie den SSH-Zugriff:

1. Wählen Sie "Device Settings" > "Device Services" (Geräteeinstellungen > Gerätedienste) aus. Die Seite "Device Service Settings" (Gerätediensteinstellungen) wird angezeigt.
2. Wählen Sie "Enable SSH Access" (SSH-Zugriff aktivieren) aus.
3. Geben Sie die SSH-Portinformationen ein. Die standardmäßige SSH-TCP-Portnummer lautet 22, sie kann jedoch geändert werden, um ein höheres Niveau für Sicherheitsvorgänge zu erreichen.
4. Klicken Sie auf OK.

HTTP- und HTTPS-Porteinstellungen

Nun können Sie von Dominion KX II verwendete HTTP- und/oder HTTPS-Ports konfigurieren. Wenn Sie z. B. den Standard-HTTP-Port 80 für andere Zwecke nutzen, wird beim Ändern des Ports sichergestellt, dass <ProdcutName> nicht versucht, diesen Port zu verwenden.

So ändern Sie die HTTP- und/oder HTTPS-Porteinstellungen:

1. Wählen Sie "Device Settings" > "Device Services" (Geräteeinstellungen > Gerätedienste) aus. Die Seite "Device Service Settings" (Gerätediensteinstellungen) wird angezeigt.
2. Geben Sie die neuen Ports in die Felder "HTTP Port" und/oder "HTTPS Port" ein.
3. Klicken Sie auf OK.

Eingeben des Erkennungsports

Die Dominion KX II-Erkennung erfolgt über einen einzelnen konfigurierbaren TCP-Port. Der Standardport lautet 5000, Sie können diesen jedoch für die Verwendung aller TCP-Ports außer 80 und 443 konfigurieren. Wenn Sie über eine Firewall auf Dominion KX II zugreifen möchten, müssen die Firewalleinstellungen die ein- und ausgehende Kommunikation über den Standardport 5000 bzw. den nicht-standardmäßigen konfigurierten Port zulassen.

So aktivieren Sie den Erkennungsport:

1. Wählen Sie "Device Settings" > "Device Services" (Geräteeinstellungen > Gerätedienste) aus. Die Seite "Device Service Settings" (Gerätediensteinstellungen) wird angezeigt.

2. Geben Sie unter "Discovery Port" (Erkennungsport) den Erkennungsport ein.
3. Klicken Sie auf OK.



Konfigurieren und Aktivieren von Schichten

Mit der Schichtfunktion können Sie über ein >ProductName<-Basisgerät auf Dominion KX II-Ziele und PDUs zugreifen. Diese Funktion ist für Dominion KX II-Standardgeräte sowie für KX2-832- und KX2-864-Geräte verfügbar. Sie können bei Bedarf maximal zwei Schichtebenen an Geräten zu einer Konfiguration hinzufügen oder aus einer Konfiguration löschen.

Beim Einrichten der Geräte verwenden Sie spezifische CIMS für spezifische Konfigurationen. Beim Einrichten der Geräte verwenden Sie spezifische CIMS für spezifische Konfigurationen. Eine Beschreibung der Ziele, die Sie in eine Schichtkonfiguration einfügen können, sowie Informationen zu CIM-Kompatibilität und Gerätekonfiguration finden Sie unter ***Schichten – Zieltypen, unterstützte CIMs und Schichtkonfigurationen*** (auf Seite 169).

Bevor Sie Schichtgeräte hinzufügen, müssen Sie die Schichten für das Basisgerät und die Schichtgeräte aktivieren. Aktivieren Sie die Basisgeräte auf der Seite "Device Settings" (Geräteeinstellungen). Aktivieren Sie die Schichtgeräte auf der Seite "Local Port Settings" (Lokale Porteinstellungen). Sobald die Geräte aktiviert und konfiguriert sind, werden Sie auf der Seite "Port Access" (Portzugriff) (***Seite "Port Access" [Portzugriff]*** (siehe "***Seite "Port Access" (Portzugriff)***" auf Seite 50)) angezeigt.

Wenn ein Dominion KX II als Basisgerät oder Schichtgerät konfiguriert wurde, wird es wie folgt angezeigt:

- Als Basisgerät konfiguriert: Dies wird im Bereich "Device Information" (Geräteinformationen) im linken Bildschirmbereich der <ProdcutName>-Oberfläche für Basisgeräte angezeigt.
- Als Schichtgerät konfiguriert: Dies wird im Bereich "Device Information" (Geräteinformationen) im linken Bildschirmbereich der <ProdcutName>-Oberfläche für Schichtgeräte angezeigt.
- Das Basisgerät wird als Basis im linken Bildschirmbereich der Schichtgerät-Oberfläche unter "Connect User" (Benutzer verbinden) identifiziert.
- Die Zielverbindungen von der Basis zu einem Schichtport werden als zwei verbundene Ports angezeigt.

Das Basisgerät ermöglicht über eine konsolidierte Portliste auf der Seite "Port Access" (Portzugriff) Remote- und lokalen Zugriff. Schichtgeräte ermöglichen Remotezugriff über ihre eigenen Portlisten. Der lokale Zugriff ist bei Schichtgeräten nicht möglich, wenn "Tiering" (Schichten) aktiviert ist.

Schichten unterstützen auch die Verwendung von KVM-Switches zum Wechseln zwischen Servern. Siehe ***Konfigurieren von KVM-Switches*** (auf Seite 189).

Aktivieren von Schichten

Verbinden Sie einen Zielserverport auf dem Basisgerät mithilfe eines D2CIM-DVUSB mit dem lokalen Port des Dominion KX II-Schichtgeräts (Video-/Tastatur-/Mausports).

Wenn es sich bei dem Schichtgerät um ein KX2-832 oder KX2-864 handelt, verbinden Sie den Zielserverport auf dem Basisgerät direkt mit dem erweiterten lokalen Port KX2-832/KX2-864 des Schichtgeräts.

► **So aktivieren Sie Schichten:**

1. Wählen Sie von der Schichtbasis "Device Settings" > "Device Services" (Geräteeinstellungen > Gerätedienste) aus. Die Seite "Device Service Settings" (Gerätediensteinstellungen) wird angezeigt.
2. Wählen Sie "Enable Tiering as Base" (Schichten als Basis aktivieren) aus.
3. Geben Sie in das Feld "Base Secret" (Geheimer Basisschlüssel) den geheimen Schlüssel ein, der von den Basis- und Schichtgeräten gemeinsam verwendet wird. Dieser geheime Schlüssel ist für die Schichtgeräte zur Authentifizierung des Basisgeräts erforderlich. Sie müssen denselben geheimen Schlüssel für das Schichtgerät eingeben.
4. Klicken Sie auf OK.
5. Aktivieren Sie die Schichtgeräte. Wählen Sie auf dem Schichtgerät "Device Settings" > "Local Port Settings" (Geräteeinstellungen > Lokale Porteinstellungen) aus.
6. Wählen Sie im Bereich "Enable Local Ports" (Lokale Ports aktivieren) die Option "Enable Local Port Device Tiering" (Lokaler Port für Geräteschichten aktivieren) aus.
7. Geben Sie im Feld "Tier Secret" (Geheimer Schlüssel der Schicht) denselben geheimen Schlüssel ein, den Sie für das Basisgerät auf der Seite "Device Settings" (Geräteeinstellungen) eingegeben haben.
8. Klicken Sie auf OK.



Schichten – Zieltypen, unterstützte CIMs und Schichtkonfigurationen

Blade-Chassis

Sie können auf direkt an die Basis angeschlossene Blade-Chassis zugreifen.

Stromzufuhrsteuerung

Sie können Ziele, die Teil einer Schichtkonfiguration sind, ein- und ausschalten. Der Zugriff auf diese Ziele erfolgt auf der Seite "Port Access" (Portzugriff).

Der Zugriff auf Dominion KX II-PDU-Ausgänge und deren Steuerung erfolgt bei >ProductName< oder den Modellen KXII-832 und KXII-864 über eine Schichtkonfiguration. Wenn Ziele und Ausgänge zugeordnet sind, steht die Stromzufuhrsteuerung auf der Seite "Port Access" (Portzugriff) zur Verfügung. Zuordnungen von Zielen und PDU-Ausgängen sind auf diejenigen beschränkt, die am selben Dominion KX II angeschlossen sind.

An Dominion KX II-Basis- oder -Schichtgeräte angeschlossene PDUs werden auf der Dropdown-Seite "Power" (Strom) zusammen mit Statistiken für den ausgewählten Powerstrip angezeigt.

Ebenso steht die Steuerung auf Ausgangsebene zur Verfügung. Sie können aktuell eingeschaltete Ausgänge ausschalten und einschalten, Sie können jedoch nicht Ausgänge ein- und ausschalten, die aktuell ausgeschaltet sind.

Dominion KX II-zu-Dominion KX II-Konfiguration oder lokale Portkonfiguration von KXII-8xx – Kompatible CIMS

Folgende CIMS sind kompatibel, wenn Sie ein Dominion KX II-Basisgerät konfigurieren, um auf zusätzliche Dominion KX II oder auf KXII-832- und KXII-864-Modelle sowie auf Dominion KX II-PDUs und Blade-Chassis zuzugreifen und diese zu steuern.

Wenn Sie eine Dominion KX II-zu-Dominion KX II-Konfiguration verwenden, müssen Sie auch D2CIM-DVUSB verwenden. Wenn Sie eine Dominion KX II-zu-KXII-8xx-Konfiguration verwenden, kann nur der erweiterte lokale Port verwendet werden.

Wenn Sie eine Konfiguration bestehend aus Dominion KX II und KXII-832 oder KXII-864 verwenden, muss die auf den Geräten ausgeführte Firmware identisch sein. Wenn Blade-Chassis Teil einer Konfiguration sind, zählt jedes Blade-Chassis als ein Zielport.

Nicht unterstützte und eingeschränkte Funktionen auf Schichtzielen

Die folgenden Funktionen werden nicht auf Schichtzielen unterstützt:

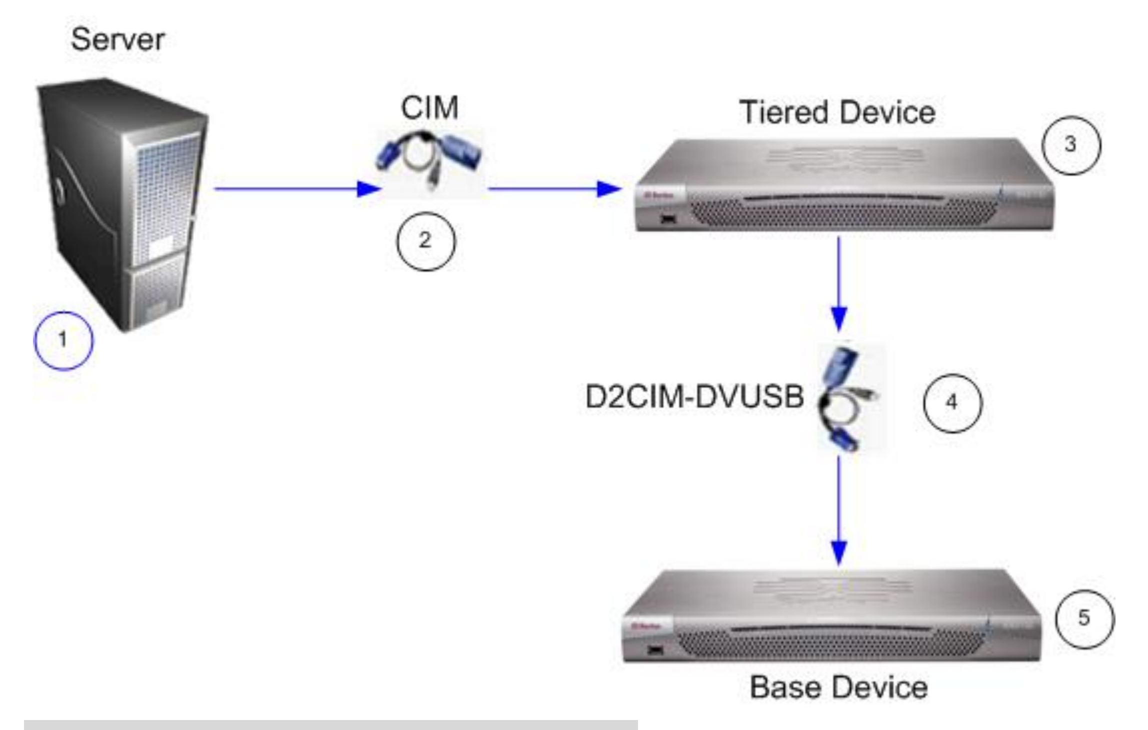
- Blade-Chassis auf Schichtgeräten
- Smartcards auf Schichtgeräten
- Virtuelle Medien von Schichtgeräten
- MCCAT als Schichtgerät

Die Portgruppenverwaltung beschränkt sich auf das Erstellen von Portgruppen mit Mitgliedern, die direkt mit der Basis verbunden sind.

Verkabelungsbeispiel in Schichtkonfigurationen

Die folgende Abbildung zeigt die Verkabelungskonfigurationen zwischen einem Dominion KX II-Schichtgerät und einem Dominion KX II-Basisgerät. Verbinden Sie einen Zielserverport auf dem Basisgerät mithilfe eines D2CIM-DVUSB mit dem lokalen Port des Dominion KX II-Schichtgeräts (Video-/Tastatur-/Mausports).

Wenn es sich bei dem Schichtgerät um ein KX2-832 oder KX2-864 handelt, verbinden Sie den Zielserverport auf dem Basisgerät direkt mit dem erweiterten lokalen Port KX2-832/KX2-864 des Schichtgeräts.



Diagrammschlüssel	
1	Zielserver
2	CIM von Zielserver zum Dominion KX II-Schichtgerät



Diagrammschlüssel	
3	Dominion KX II-Schichtgerät
4	D2CIM-DVUSB CIM vom Dominion KX II-Schichtgerät zum Dominion KX II-Basisgerät
5	Dominion KX II-Basisgerät

Aktivieren des direkten Port-Zugriffs

Der direkte Portzugriff ermöglicht es Benutzern, die Verwendung der Seite "Login dialog and Port Access" (Anmeldedialog und Port-Zugriff) zu umgehen. Diese Funktion bietet auch die Möglichkeit, Benutzername und Kennwort direkt einzugeben und das Ziel aufzurufen, wenn Benutzername und Kennwort nicht in der URL enthalten sind.

Wichtige URL-Informationen für den direkten Portzugriff:

Wenn Sie den VKC und direkten Port-Zugriff verwenden:

- https://IP-Adresse/dpa.asp?username=Benutzername&password=Kennwort&port=Port-Nummer

Wenn Sie den AKC und direkten Port-Zugriff verwenden:

- https://IP-Adresse/dpa.asp?username=Benutzername&password=Kennwort&port=Portnummer&client=akc

Dabei gilt:

- Benutzername und Kennwort sind optional. Werden Sie nicht bereitgestellt, wird ein Dialogfeld für die Anmeldung angezeigt. Nach der Authentifizierung wird der Benutzer direkt mit dem Ziel verbunden.
- Für den Port kann eine Port-Nummer oder ein Port-Name angegeben sein. Wenn Sie einen Port-Namen verwenden, muss dieser eindeutig sein, sonst wird ein Fehler gemeldet. Bleibt der Port unberücksichtigt, wird ein Fehler gemeldet.
- Der festgelegte Port für Blade-Chassis lautet: <port number>-<slot number>. Blade-Chassis, die mit Port 1 und Slot 2 verbunden sind, werden mit 1-2 angegeben.
- "Client=akc" ist optional, außer Sie verwenden den AKC. Wird "Client=akc" nicht verwendet, wird der VKC verwendet.

▸ So aktivieren Sie den direkten Port-Zugriff:

1. Wählen Sie "Device Settings" > "Device Services" (Geräteeinstellungen > Gerätedienste) aus. Die Seite "Device Service Settings" (Gerätediensteinstellungen) wird angezeigt.



2. Aktivieren Sie die Option "Enable Direct Port Access via URL" (Direkten Port-Zugriff über URL aktivieren), wenn Sie möchten, dass Benutzer über Dominion KX II durch Eingabe der erforderlichen Parameter in die URL direkten Zugriff auf ein Ziel haben.
3. Klicken Sie auf OK.

Aktivieren der AKC-Download-Serverzertifikat-Validierung

Wenn Sie den AKC verwenden, können Sie wählen, ob Sie die Funktion "Enable AKC Download Server Certificate Validation" (AKC-Download-Serverzertifikat-Validierung aktivieren) verwenden möchten oder nicht.

Option 1: Do Not Enable AKC Download Server Certificate Validation (AKC-Download-Serverzertifikat-Validierung nicht aktivieren [Standardeinstellung])

Wenn Sie die AKC-Download-Serverzertifikat-Validierung nicht aktivieren, müssen alle KX II-Benutzer und CC-SG Bookmark- und Access-Client-Benutzer:

- Stellen Sie sicher, dass die Cookies von der IP-Adresse des Geräts, auf das zugegriffen wird, nicht blockiert werden.
- Die Benutzer von Windows Vista-, Windows 7- und Windows 2008-Servern müssen sicherstellen, dass die IP-Adresse des Geräts, auf das zugegriffen wird, in der Zone "Vertrauenswürdige Sites" hinzugefügt wurde und dass der "Geschützte Modus" nicht aktiv ist, wenn auf das Gerät zugegriffen wird.

Option 2: Enable AKC Download Server Certificate Validation (Übersicht zur AKC-Download-Serverzertifikat-Validierung aktivieren)

Wenn Sie die AKC-Download-Serverzertifikat-Validierung aktivieren:

- Administratoren müssen ein gültiges Zertifikat zu Dominion KX II hochladen oder ein selbstsigniertes Zertifikat auf Dominion KX II generieren. Das Zertifikat muss über eine gültige Hostbezeichnung verfügen.
- Jeder Benutzer muss das CA-Zertifikat (oder eine Kopie des selbstsignierten Zertifikats) zum Speicher für "Vertrauenswürdige Stammzertifizierungsstellen" seines Browsers hinzufügen.

▶ So installieren Sie das selbstsignierte Zertifikat unter Windows Vista® oder Windows 7®:

1. Fügen Sie die Dominion KX II-IP-Adresse in der Zone "Vertrauenswürdige Sites" hinzu, und stellen Sie sicher, dass der "Geschützte Modus" nicht aktiv ist.



2. Starten Sie Internet Explorer®, und geben Sie die Dominion KX II-IP-Adresse als URL ein. Eine Meldung "Zertifikatfehler" wird angezeigt.
3. Wählen Sie "Zertifikate anzeigen" aus.
4. Klicken Sie auf der Registerkarte "Allgemein" auf "Zertifikat installieren". Das Zertifikat wird dann zum Speicher für "Vertrauenswürdige Stammzertifizierungsstellen" hinzugefügt.
5. Nachdem das Zertifikat installiert wurde, kann die Dominion KX II-IP-Adresse aus der Zone für "Vertrauenswürdige Sites" entfernt werden.

So aktivieren Sie die AKC-Download-Serverzertifikat-Validierung:

1. Wählen Sie "Device Settings" > "Device Services" (Geräteeinstellungen > Gerätedienste) aus. Die Seite "Device Service Settings" (Gerätediensteinstellungen) wird angezeigt.
2. Aktivieren oder deaktivieren (Standardeinstellung) Sie das Kontrollkästchen "Enable AKC Download Server Certificate Validation" (AKC-Download-Serverzertifikat-Validierung).
3. Klicken Sie auf OK.

Konfigurieren der Modemeinstellungen

So konfigurieren Sie Modemeinstellungen:

1. Klicken Sie auf "Device Settings" > "Modem Settings" (Geräteeinstellungen > Modemeinstellungen), um die Seite "Modem Settings" (Modemeinstellungen) zu öffnen.
2. Aktivieren Sie das Kontrollkästchen "Enable Modem" (Modem aktivieren). Dadurch werden die Felder "Serial Line Speed" (Geschwindigkeit der seriellen Verbindung) und "Modem Init String" (String für Modeminitialisierung) aktiviert.
3. Die Geschwindigkeit der seriellen Verbindung des Modems ist auf 115200 eingestellt. **Schreibgeschützt**
4. Geben Sie im Feld "Modem Init String" (String für Modeminitialisierung) die Standardzeichenfolge des Modems ein. Wenn das Feld für die Modemzeichenfolge leer bleibt, wird standardmäßig die folgende Zeichenfolge an das Modem gesendet: ATZ OK AT OK.

Diese Informationen werden für die Konfiguration der Modemeinstellungen verwendet. Da bei verschiedenen Modems diese Werte auf unterschiedliche Art eingestellt werden, wird in diesem Dokument nicht angegeben, wie diese Werte festgelegt werden. Informationen zum Erstellen der entsprechenden modemspezifischen Zeichenfolge finden Sie in den Unterlagen Ihres Modems.

- Modemeinstellungen:
- RTS/CTS-Flusssteuerung aktivieren
- Bei Empfang von RTS Daten an den Computer senden
- CTS sollte so konfiguriert sein, dass die Verbindung nur getrennt wird, wenn die Flusssteuerung dies erforderlich macht.
- DTR sollte für Modem-Rücksetzungen mit DTR-Toggle konfiguriert werden.
- DSR sollte immer als "Ein" konfiguriert werden.
- DCD sollte nach Erkennen eines Trägersignals als "Aktiviert" konfiguriert werden (d. h. DCD sollte nur aktiviert werden, wenn eine Modemverbindung mit dem Remotegerät hergestellt wurde).

5. Geben Sie die Modemserver-IPv4-Adresse in das Feld "Modem Server IPv4 Address" (Modemserver-IPv4-Adresse) und die Client-Modemadresse in das Feld "Modem Client IPv4 Address" (Modemclient-IPv4-Adresse) ein.

Hinweis: Die Modemclient- und Server-IP-Adressen müssen sich im gleichen Subnetz befinden und dürfen sich nicht mit dem KX LAN-Subnetz überschneiden.



6. Klicken Sie auf OK, um Ihre Änderungen zu bestätigen, oder klicken Sie auf "Reset to Defaults" (Auf Standardeinstellungen zurücksetzen), um die Einstellungen auf die Standartwerte zurückzusetzen.



Weitere Informationen zu zertifizierten Modems, die von Dominion KX II unterstützt werden, finden Sie unter ***Zertifizierte Modems*** (auf Seite 321). Informationen zu Einstellungen für optimale Leistung bei der Verbindung mit Dominion KX II über ein Modem finden Sie im Abschnitt "Creating, Modifying and Deleting Profiles in MPC - Generation 2 Devices" (Erstellen, Ändern und Löschen von Profilen im MPC – Geräte der 2. Generation) des Benutzerhandbuchs **KVM and Serial Access Clients Guide**.

Hinweis: Der direkte Modemzugriff auf die HTML-Oberfläche des Dominion KX II wird nicht unterstützt. Um über ein Modem auf Dominion KX II zuzugreifen, müssen Sie eine eigenständige MPC-Anwendung verwenden.



Konfigurieren von Datum-/Uhrzeiteinstellungen

Auf der Seite "Date/Time Settings" (Datum-/Uhrzeiteinstellungen) stellen Sie Datum und Uhrzeit für Dominion KX II ein. Hierzu haben Sie zwei Möglichkeiten:

- Datum und Uhrzeit manuell einstellen
- Datum und Uhrzeit mit einem NTP (Network Time Protocol)-Server synchronisieren

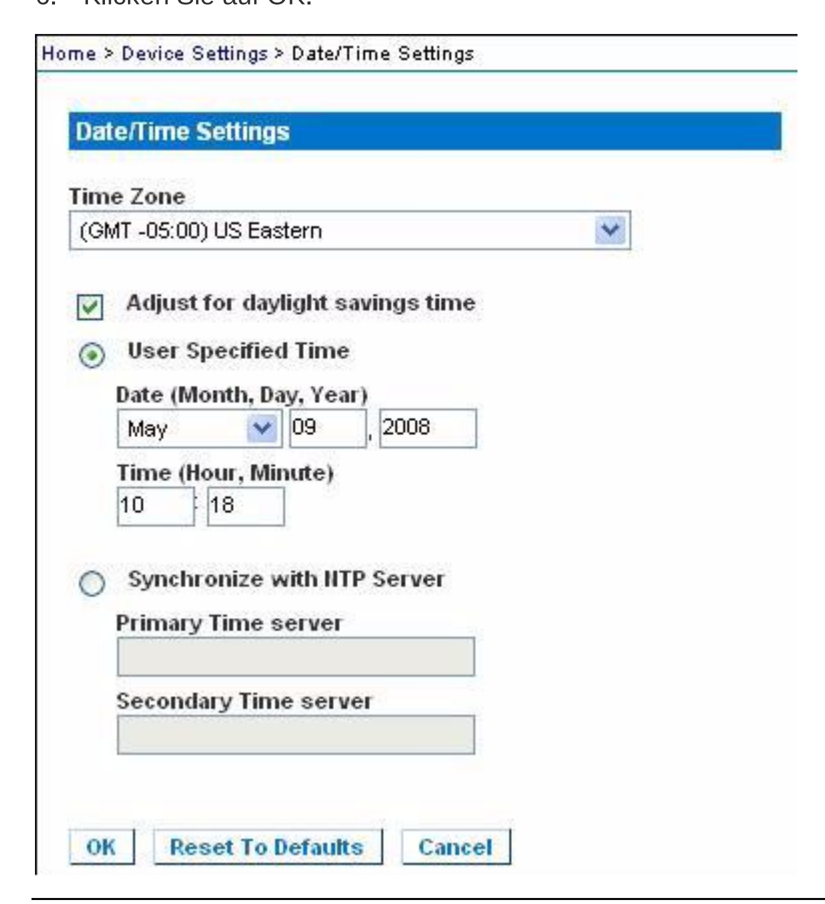
So stellen Sie das Datum und die Uhrzeit ein:

1. Wählen Sie "Device Settings" > "Date/Time" (Geräteeinstellungen > Datum/Uhrzeit) aus. Die Seite "Date/Time Settings" (Datum-/Uhrzeiteinstellungen) wird angezeigt.
2. Wählen Sie in der Dropdownliste "Time Zone" Ihre Zeitzone aus.
3. Aktivieren Sie das Kontrollkästchen "Adjust for daylight savings time" (an Sommerzeit anpassen), um die Uhrzeit an die Sommerzeit anzupassen.
4. Wählen Sie eine Methode, um Datum und Uhrzeit einzustellen:
   - User Specified Time (Benutzerdefinierte Zeit) – Bei dieser Option können Sie Datum und Uhrzeit manuell eingeben.

     Falls Sie die Option "User Specified Time" (Benutzerdefinierte Zeit) ausgewählt haben, geben Sie Datum und Uhrzeit wie folgt ein: Geben Sie im Feld "Time" die Uhrzeit im Format hh:mm ein. (Verwenden Sie das 24-h-Zeitformat.)
   - Synchronize with NTP Server (Mit NTP-Server synchronisieren) – Bei dieser Option können Sie Datum und Uhrzeit mit dem NTP (Network Time Protocol)-Server synchronisieren.
5. Falls Sie die Option "Synchronize with NTP Server" (Mit NTP-Server synchronisieren) ausgewählt haben, gehen Sie folgendermaßen vor:
   a. Geben Sie im Feld "Primary Time Server" (Primärer Zeitserver) die IP-Adresse dieses Servers ein.
   b. Geben Sie im Feld "Secondary Time Server" (Sekundärer Zeitserver) die IP-Adresse dieses Servers ein. **Optional**



6. Klicken Sie auf OK.



Hinweis: Sowohl IPv4- als auch IPv6-Adressen werden unterstützt.

Ereignisverwaltung

Das Dominion KX II-Feature zur Ereignisverwaltung bietet eine Reihe von Fenstern, in denen Sie die Verteilung von Systemereignissen auf SNMP-Manager, Syslog und das Prüfprotokoll aktivieren und deaktivieren können. Die Ereignisse werden kategorisiert, und Sie können für jedes Ereignis festlegen, ob es an eines oder mehrere Ziele gesendet werden soll.

Event Management - Settings (Konfigurieren der Ereignisverwaltung – Einstellungen)

SNMP-Konfiguration

Simple Network Management Protocol (SNMP) ist ein Protokoll für die Netzwerkverwaltung und die Überwachung von Netzwerkgeräten und ihrer Funktionen. Dominion KX II bietet über die Ereignisverwaltung Unterstützung für SNMP-Agenten.

- **So konfigurieren Sie SNMP (und aktivieren die SNMP-Protokollierung):**

1. Wählen Sie "Device Settings" > "Event Management - Settings" (Geräteeinstellungen > Ereignisverwaltung – Einstellungen) aus. Die Seite "Event Management - Settings" (Ereignisverwaltung – Einstellungen) wird angezeigt.
2. Wählen Sie "SNMP Logging Enabled" (SNMP-Protokollierung aktiviert) aus. Dadurch werden die übrigen SNMP-Felder aktiviert.
3. Geben Sie in die Felder "Name", "Contact" (Kontakt) und "Location" (Ort) den Namen des SNMP-Agenten (der Name des Geräts), wie er in der Dominion KX II-Konsolenoberfläche angezeigt wird, einen Kontaktnamen für dieses Gerät und den physischen Ort des Dominion-Geräts ein.
4. Geben Sie im Feld "Agent Community String" (Community-String des Agenten) die Zeichenfolge des Geräts ein. Eine SNMP-Community ist die Gruppe, der Geräte und Verwaltungsstationen angehören, auf denen SNMP ausgeführt wird. Durch sie können Sie leichter definieren, wohin Informationen gesendet werden. Der Community-Name wird zur Identifizierung der Gruppe verwendet. Das SNMP-Gerät oder der SNMP-Agent kann zu mehreren SNMP-Communities gehören.
5. Legen Sie über die Dropdownliste "Type" (Typ) den Lesezugriff (Read-Only) oder den Lese-/Schreibzugriff (Read-Write) für die Community fest.
6. Konfigurieren Sie maximal fünf SNMP-Manager, indem Sie entsprechende Werte in die Felder "Destination IP/Host Name" (IP-Zieladresse/Hostname), "Port #" (Portnummer) und "Community" eingeben.
7. Klicken Sie auf den Link "Click here to view the Dominion SNMP MIB" (Klicken Sie hier, um die Dominion-SNMP MIB anzuzeigen), um auf die SNMP Management Information Base zuzugreifen.
8. Klicken Sie auf OK.



So konfigurieren Sie Syslog und aktivieren die Weiterleitung:

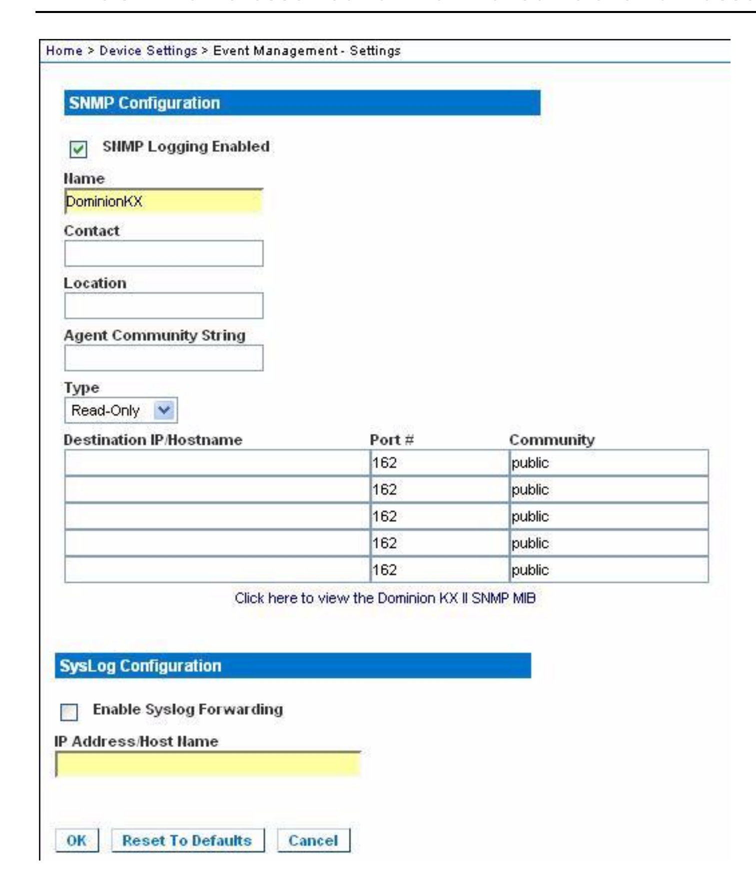
1. Wählen Sie "Enable Syslog Forwarding" (Syslog-Weiterleitung aktivieren) aus, um Geräte-Protokollmeldungen an einen Remote-Syslog-Server zu senden.
2. Geben Sie die IP-Adresse bzw. den Hostnamen Ihres Syslog-Servers im Feld "IP Address" (IP-Adresse) ein.
3. Klicken Sie auf OK.

So kehren Sie zu den Werkseinstellungen zurück:

- Klicken Sie auf "Reset to Defaults" (Standardeinstellungen wiederherstellen).

Hinweis: Sowohl IPv4- als auch IPv6-Adressen werden unterstützt.

Hinweis: IPv6-Adressen dürfen maximal 80 Zeichen umfassen.





Event Management - Destinations (Ereignisverwaltung – Ziele)

Systemereignisse können (falls aktiviert) SNMP-Benachrichtigungsereignisse (Traps) generieren oder in Syslog oder dem Prüfprotokoll protokolliert werden. Auf der Seite "Event Management - Destinations" (Ereignisverwaltung – Ziele) legen Sie fest, welche Systemereignisse verfolgt und wohin diese Informationen gesendet werden sollen.

Hinweis: SNMP-Traps werden nur erzeugt, wenn die Option "SNMP Logging Enabled" (SNMP-Protokollierung aktivieren) ausgewählt ist. Syslog-Ereignisse werden nur erzeugt, wenn die Option "Enable Syslog Forwarding" (Syslog-Weiterleitung aktivieren) ausgewählt ist. Beide Optionen befinden sich auf der Seite "Event Management - Settings" (Ereignisverwaltung - Einstellungen). Siehe Configuring Event Management - Settings (Konfigurieren der Ereignisverwaltung – Einstellungen).

So wählen Sie Ereignisse und ihr Ziel aus:

1. Wählen Sie "Device Settings" > "Event Management - Destinations" (Geräteeinstellungen > Ereignisverwaltung – Ziele) aus. Die Seite "Event Management - Destinations" (Ereignisverwaltung – Ziele) wird angezeigt.

   Die Systemereignisse sind nach "Device Operation" (Gerätebetrieb), "Device Management" (Geräteverwaltung), "Security" (Sicherheit), "User Activity" (Benutzeraktivität) und "User Group Administration" (Benutzergruppenverwaltung) kategorisiert.

2. Aktivieren Sie die Kontrollkästchen der Ereignisse, die Sie aktivieren bzw. deaktivieren möchten, und geben Sie an, wohin die Informationen gesendet werden sollen.

   Tipp: Ganze Kategorien können durch Aktivieren bzw. Deaktivieren der entsprechenden Kategorie-Kontrollkästchen aktiviert bzw. deaktiviert werden.



3. Klicken Sie auf OK.

Home > Device Settings > Event Management - Destinations | Logout

Event Management - Destinations

Note: SNMP traps will only be generated if the "SNMP Logging Enabled" option is checked. Similarly, Syslog events will only be generated if the "Enable Syslog Forwarding" option is checked. These options can be found on the "Event Management - Settings" page on the Device Settings menu.

Category	Event	SNMP	Syslog	Audit Log
Device Operation		☑	☑	☑
	System Startup	☑	☑	☑
	System Shutdown	☑	☑	☑
	Power Supply Status Changed	☑	☑	☑
	Powerstrip Outlet Status Changed	☑	☑	☑
	Network Parameter Changed	☑	☑	☑
	Port Status Changed	☑	☑	☑
	Network Failure			☑
	Ethernet Failover	☑	☑	☑
Device Management		☑	☑	☑
	FactoryReset	☑	☑	☑
	Begin CC Control	☑	☑	☑
	End CC Control	☑	☑	☑
	Device Update Started	☑	☑	☑
	Device Update Completed	☑	☑	☑
	Device Update Failed	☑	☑	☑
	Firmware Update Failed	☑	☑	☑
	Firmware File Discarded	☑	☑	☑
	Firmware Validation Failed	☑	☑	☑
	Configuration Backed Up	☑	☑	☑
	Configuration Restored	☑	☑	☑
	Port Connection Denied	☑	☑	☑
Security		☑	☑	☑
	Password Settings Changed	☑	☑	☑
	Login Failed	☑	☑	☑
	Password Changed	☑	☑	☑
	User Blocked		☑	☑
User Activity		☑	☑	☑
	Port Connected	☑	☑	☑
	Port Disconnected	☑	☑	☑

So kehren Sie zu den Werkseinstellungen zurück:

- Klicken Sie auf "Reset to Defaults" (Standardeinstellungen wiederherstellen).

Warnung: Bei der Verwendung von SNMP-Traps über UDP kann die Synchronisierung zwischen Dominion KX II und dem damit verbundenen Router verloren gehen, wenn Dominion KX II neu gestartet wird. Das SNMP-Trap Reboot Completed" (Neustart abgeschlossen) wird dadurch nicht protokolliert.

SNMP-Agent-Konfiguration

SNMP-kompatible Geräte, genannt Agenten, speichern Daten über sich selbst in Management Information Bases (MIBs) und geben diese Daten an die SNMP-Manager zurück. Auf der Seite "Event Logging" (Ereignisprotokollierung) können Sie die SNMP-Verbindung zwischen Dominion KX II (SNMP-Agent) und einem SNMP-Manager konfigurieren.

SNMP-Trap-Konfiguration

SNMP bietet die Möglichkeit, Traps (Benachrichtigungen) zu senden, um einen Administrator zu informieren, wenn eine oder mehrere Bedingungen erfüllt sind. Die folgende Tabelle enthält die SNMP-Traps von Dominion KX II:

Trap-Name	Beschreibung
bladeChassisCommError	Es wurde ein Kommunikationsfehler bei einem an diesen Port angeschlossenen Blade-Chassis-Gerät festgestellt. *Hinweis: Nicht vom Modell KX II-101 unterstützt.*
configBackup	Die Gerätekonfiguration wurde gesichert.
configRestore	Die Gerätekonfiguration wurde wiederhergestellt.
deviceUpdateFailed	Das Gerät konnte nicht aktualisiert werden.
deviceUpgradeCompleted	Dominion KX II hat die Aktualisierung mittels einer RFP-Datei abgeschlossen.
deviceUpgradeStarted	Dominion KX II hat die Aktualisierung mittels einer RFP-Datei begonnen.
factoryReset	Das Gerät wurde auf die Werkseinstellungen zurückgesetzt.
firmwareFileDiscarded	Die Firmwaredatei wurde verworfen.
firmwareUpdateFailed	Die Firmware konnte nicht aktualisiert werden.
firmwareValidationFailed	Die Firmware konnte nicht validiert werden.



Trap-Name	Beschreibung
groupAdded	Eine Gruppe wurde zum Dominion KX II-System hinzugefügt.
groupDeleted	Eine Gruppe wurde aus dem System gelöscht.
groupModified	Eine Gruppe wurde geändert.
ipConflictDetected	Ein IP-Adressenkonflikt wurde erkannt.
ipConflictResolved	Ein IP-Adressenkonflikt wurde gelöst.
networkFailure	Für eine der Ethernet-Schnittstellen des Produkts besteht keine Netzwerkverbindung mehr.
networkParameterChanged	Die Netzwerkparameter wurden geändert.
passwordSettingsChanged	Die Einstellungen für sichere Kennwörter wurden geändert.
portConnect	Ein zuvor authentifizierter Benutzer hat eine KVM-Sitzung gestartet.
portConnectionDenied	Eine Verbindung mit dem Zielport wurde verweigert.
portDisconnect	Die Sitzung des Benutzers einer KVM-Sitzung wird von selbigem ordnungsgemäß geschlossen.
portStatusChange	Der Port ist nicht mehr verfügbar.
powerNotification	Benachrichtigung über den Status der Stromversorgung: 1 = Aktiv, 0 = Inaktiv.
powerOutletNotification	Benachrichtigung über den Status eines Powerstrip-Geräteausgangs.
rebootCompleted	Der Neustart von Dominion KX II ist abgeschlossen.
rebootStarted	Dominion KX II wird neu gestartet: entweder durch Wiederherstellen der Stromversorgung oder durch einen "Warmstart" mittels des Betriebssystems.
securityViolation	Ein Sicherheitsproblem ist aufgetreten.
startCCManagement	Für das Gerät wurde die CommandCenter-Verwaltung gestartet.
stopCCManagement	Die CommandCenter-Verwaltung des Geräts wurde aufgehoben.
userAdded	Ein Benutzer wurde zum System hinzugefügt.
userAuthenticationFailure	Ein Benutzer hat versucht, sich mit einem falschen Benutzernamen und/oder Kennwort anzumelden.
userConnectionLost	Bei einem Benutzer mit aktiver Sitzung ist eine nicht ordnungsgemäße Sitzungstrennung

Trap-Name	Beschreibung
	aufgetreten.
userDeleted	Ein Benutzerkonto wurde gelöscht.
userForcedLogout	Ein Benutzer wurde durch "Admin" zwangsabgemeldet.
userLogin	Ein Benutzer hat sich erfolgreich bei Dominion KX II angemeldet und wurde authentifiziert.
userLogout	Ein Benutzer hat sich erfolgreich und ordnungsgemäß von Dominion KX II abgemeldet.
userModified	Ein Benutzerkonto wurde geändert.
userPasswordChanged	Das Ereignis wird ausgelöst, wenn das Kennwort eines Benutzers des Geräts geändert wird.
userSessionTimeout	Die aktive Sitzung eines Benutzers wurde aufgrund einer Zeitüberschreitung beendet.
userUploadedCertificate	Ein Benutzer hat ein SSL-Zertifikat hochgeladen.
vmImageConnected	Ein Benutzer hat versucht, ein Gerät oder ein Abbild mithilfe virtueller Medien auf dem Zielgerät zu installieren. Für jeden Versuch einer Geräte-/Abbildzuordnung (Installation) wird dieses Ereignis generiert.
vmImageDisconnected	Ein Benutzer hat versucht, ein Gerät oder ein Abbild mithilfe virtueller Medien auf dem Zielgerät zu deinstallieren.

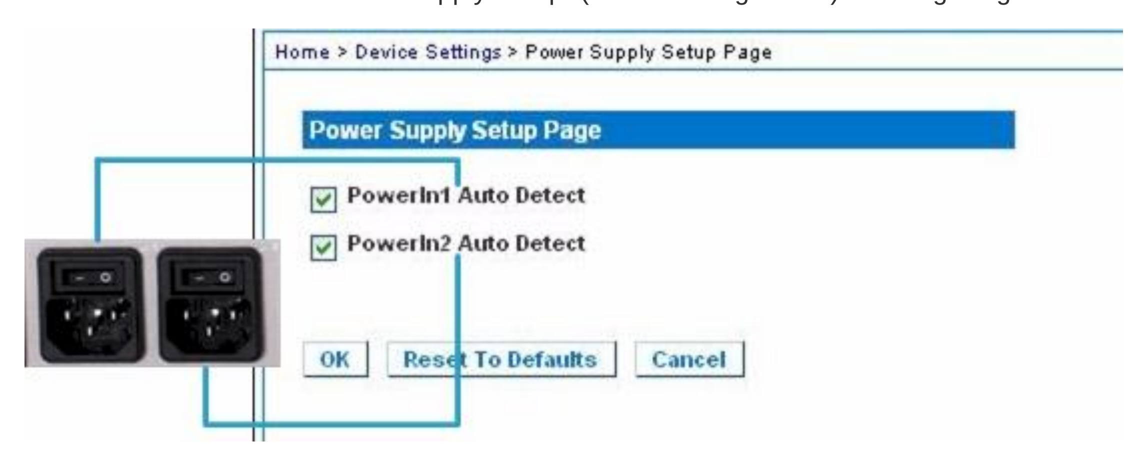


Netzteilkonfiguration

Dominion KX II bietet zwei Netzteile und kann den Status dieser Netzteile automatisch erkennen und entsprechende Benachrichtigungen ausgeben. Geben Sie auf der Seite "Power Supply Setup" (Netzteilkonfiguration) an, ob Sie eines oder beide Netzteile verwenden. Mit der korrekten Konfiguration stellen Sie sicher, dass Dominion KX II die entsprechenden Benachrichtigungen bei einem Ausfall der Stromversorgung sendet. Wenn beispielsweise Netzteil 1 ausfällt, leuchtet die Stromversorgungs-LED-Anzeige auf der Vorderseite der Einheit rot.

So aktivieren Sie die automatische Erkennung für die verwendeten Netzteile:

1. Wählen Sie "Device Settings > Power Supply Setup" (Geräteeinstellungen und Netzteilkonfiguration) aus. Die Seite "Power Supply Setup" (Netzteilkonfiguration) wird angezeigt.



2. Wenn Sie den Strom über das Netzteil 1 zuführen (ganz links auf der Rückseite des Geräts), wählen Sie die Option "PowerIn1 Auto Detect" (Netzteil 1 – Automatische Erkennung) aus.
3. Wenn Sie den Strom über das Netzteil 2 zuführen (ganz rechts auf der Rückseite des Geräts), wählen Sie die Option "PowerIn2 Auto Detect" (Netzteil 2 – Automatische Erkennung) aus.
4. Klicken Sie auf OK.

Hinweis: Wenn eines dieser Kontrollkästchen aktiviert ist und das entsprechende Netzteil zurzeit nicht angeschlossen ist, leuchtet die Stromversorgungs-LED-Anzeige auf der Vorderseite der Einheit rot.

So deaktivieren Sie die automatische Erkennung:

- Deaktivieren Sie das Kontrollkästchen für das entsprechende Netzteil.

So kehren Sie zu den Werkseinstellungen zurück:

- Klicken Sie auf die Schaltfläche **Reset To Defaults** (Standardeinstellungen wiederherstellen).

Hinweis: Dominion KX II übermittelt den Status der Netzteile NICHT an CommandCenter. Dominion I (Generation 1) hingegen tut dies.

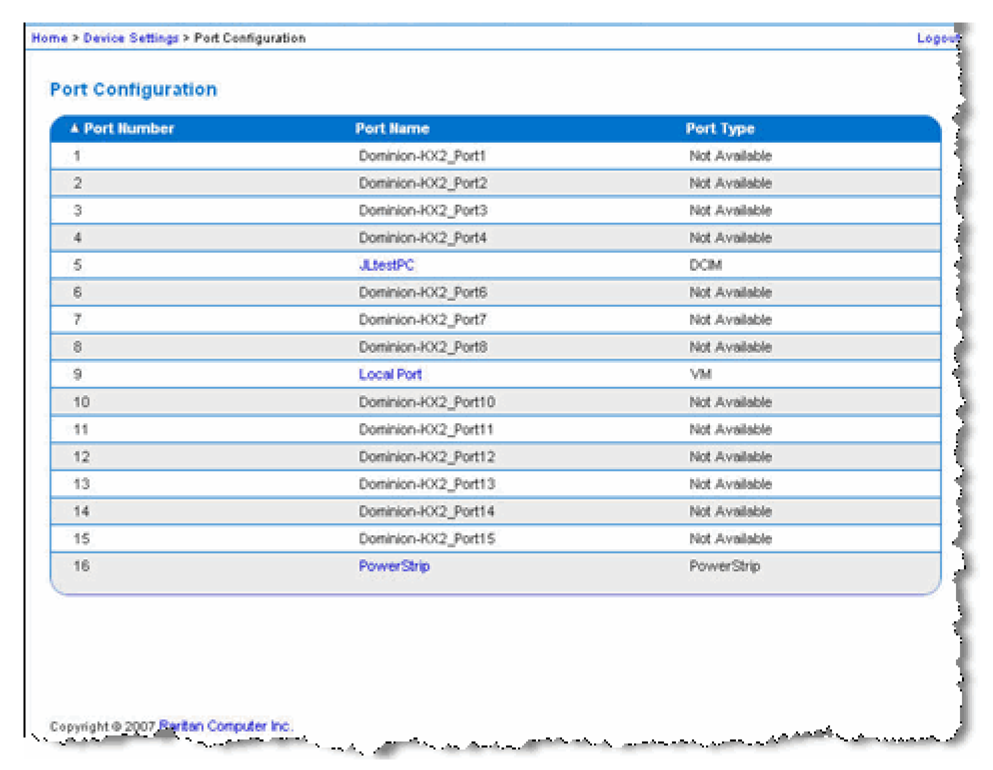


Konfiguration von Ports

Die Seite "Port Configuration" (Portkonfiguration) enthält eine Liste der Dominion KX II-Ports. Ports, die mit KVM-Zielservern (Blade- oder Standardserver) und Powerstrips verbunden sind, werden blau angezeigt und können bearbeitet werden. Ports, an die kein CIM angeschlossen oder für die kein CIM-Name angegeben ist, wird der Standardportname "Dominion-KX2_Port#" zugewiesen, wobei "Port#" für die Nummer des physischen Dominion KX II-Ports steht.

▶ So greifen Sie auf eine Portkonfiguration zu:

1. Wählen Sie "Device Settings" > "Port Configuration" (Geräteeinstellungen > Portkonfiguration) aus. Die Seite "Port Configuration" (Portkonfiguration) wird angezeigt.



Der Inhalt der Seite wird zunächst in der Reihenfolge der Portnummern angezeigt. Sie können für eine andere Sortierung jedoch auf eine der Spaltenüberschriften klicken.

- Port Number (Portnummer) – Die für das Dominion KX II-Gerät verfügbaren Ports werden beginnend mit 1 durchnummeriert.
- Port Name (Portname) – Der dem Port zugewiesene Name. Ein schwarzer Portname gibt an, dass Name und Port nicht geändert bzw. bearbeitet werden können. Blaue Portnamen können dagegen bearbeitet werden.

Hinweis: Verwenden Sie für den Port (CIM)-Namen keine Auslassungszeichen (Apostroph).

- Port Type (Porttyp)

Porttyp	Beschreibung
DCIM	Dominion CIM
Not Available (Nicht verfügbar)	Kein CIM angeschlossen
PCIM	Paragon CIM
PowerStrip	Power CIM
VM	Virtuelle Medien-CIM (D2CIM-VUSB und D2CIM-DVUSB)
Blade-Chassis	Blade-Chassis und die dem Chassis zugeordneten Blades (in hierarchischer Reihenfolge angezeigt)

2. Klicken Sie auf den Portnamen des Ports, den Sie bearbeiten möchten.
   - Bei KVM-Ports wird die Seite "Port" angezeigt. Auf dieser Seite können Sie die Ports benennen und Stromzuordnungen erstellen.
   - Bei Powerstrips wird die Portseite für Powerstrips angezeigt. Auf dieser Seite können Sie die Powerstrips und die Ausgänge benennen.

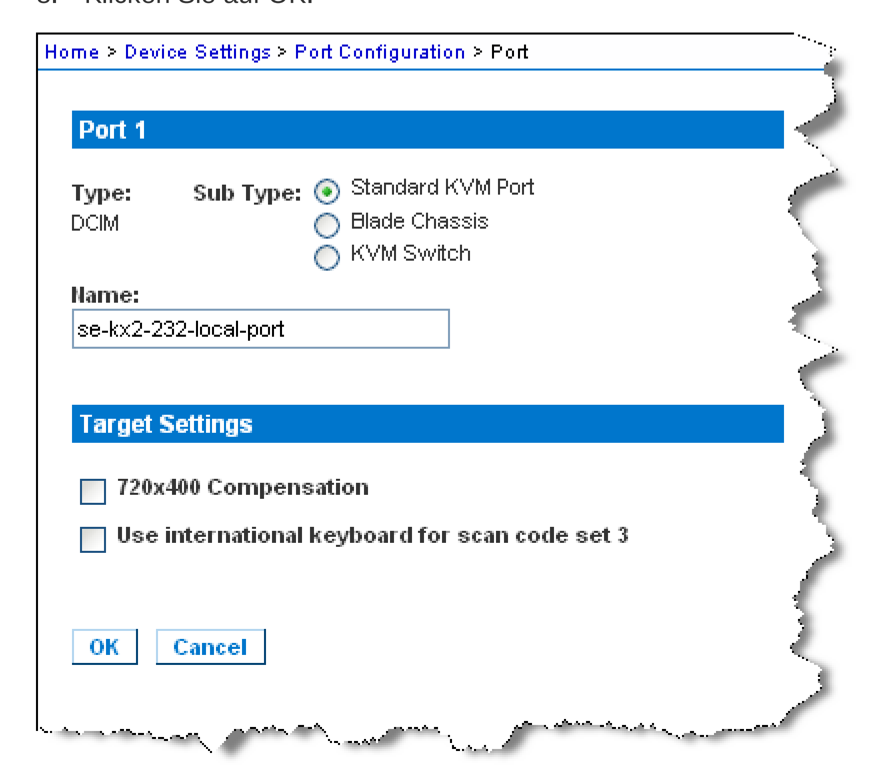
Konfigurieren von Standardzielservern

So benennen Sie die Zielserver:

1. Schließen Sie alle Zielserver an, falls dies noch nicht geschehen ist. Weitere Einzelheiten finden Sie unter ***Schritt 3: Anschließen der Geräte*** (siehe "***Schritt 3: Anschließen der Geräte***" auf Seite 30) für eine Beschreibung zum Anschließen der Geräte.
2. Wählen Sie "Device Settings" > "Port Configuration" (Geräteeinstellungen > Portkonfiguration) aus. Die Seite "Port Configuration" (Portkonfiguration) wird angezeigt.
3. Klicken Sie auf den Portnamen des Zielservers, den Sie umbenennen möchten. Die Seite "Port" wird angezeigt.
4. Weisen Sie dem mit diesem Port verbundenen Server einen Namen zu. Der Name darf maximal 32 alphanumerische Zeichen oder Sonderzeichen umfassen.
5. Wählen Sie "Standard KVM Port" als Subtyp für den Port aus.



6. Wählen Sie im Bereich "Target Settings" (Zieleinstellungen) die Option "720x400 Compensation" (720x400-Kompensierung) aus, wenn das Ziel diese Auflösung verwendet und Anzeigeprobleme auftreten.
7. Wählen Sie "Use international keyboard for scan code set 3" (Internationale Tastatur für Scancode Satz 3 verwenden) aus, wenn Sie mit einem DCIM-PS2 die Verbindung zum Ziel herstellen und den Scancode Satz 3 mit einer internationalen Tastatur verwenden müssen.
8. Klicken Sie auf OK.



Konfigurieren von KVM-Switches

Dominion KX II unterstützt außerdem die Verwendung von Tastenfolgen, um zwischen Zielen zu wechseln. Außer der Verwendung von Tastenfolgen mit Standardservern wird KVM-Switching auch von Blade-Chassis und Schichtkonfigurationen unterstützt.

So konfigurieren Sie KVM-Switches:

1. Wählen Sie "Device Settings" > "Port Configuration" (Geräteeinstellungen > Portkonfiguration) aus. Die Seite "Port Configuration" (Portkonfiguration) wird angezeigt.
2. Klicken Sie auf den Portnamen des Zielservers, den Sie umbenennen möchten. Die Seite "Port" wird angezeigt.

3. Wählen Sie den KVM-Switch aus.
4. Wählen Sie das KVM-Switch-Modell aus.

Hinweis: Es wird nur ein Switch in der Dropdown-Liste angezeigt.

5. Wählen Sie "KVM Switch Hot Key Sequence" (KVM-Switch-Tastenfolge) aus.
6. Geben Sie die maximale Anzahl der Zielports (2-32) ein.
7. Geben Sie im Feld "KVM Switch Name" den gewünschten Namen für diese Portkonfiguration ein.
8. Aktivieren Sie die Ziele für die KVM-Switch-Tastenfolge. Geben Sie die KVM-Switch-Ports mit angeschlossenen Zielen an, indem Sie für jeden Port "Active" (Aktiv) auswählen.
9. Im Abschnitt "KVM Managed Links" (Verwaltete KVM-Verknüpfungen) der Seite können Sie die Verbindung zu einer Webbrowseroberfläche konfigurieren, wenn verfügbar.
   a. Active (Aktiv) – Aktivieren Sie das Kontrollkästchen "Active" (Aktiv), um die Verknüpfung nach der Konfiguration zu aktivieren. Aktiveren Sie das Kontrollkästchen nicht, wenn die Verknüpfung inaktiv bleiben soll. In die Verknüpfungsfelder können Informationen auch dann eingegeben und gespeichert werden, wenn "Active" (Aktiv) nicht ausgewählt wurde. Wenn "Active" (Aktiv) ausgewählt wurde, muss im URL-Feld eine Eingabe vorgenommen werden. Benutzername, Kennwort sowie die Felder "Username" (Benutzername) und "Password" (Kennwort) sind optional (abhängig davon, ob eine Einzelanmeldung gewünscht wird oder nicht).
   b. URL Name – Geben Sie die URL zur Benutzeroberfläche ein.
   c. Username (Benutzername) – Geben Sie den Benutzernamen ein, der für den Zugriff auf die Benutzeroberfläche verwendet wird.
   d. Password (Kennwort) – Geben Sie das Kennwort ein, das für den Zugriff auf die Benutzeroberfläche verwendet wird.
   e. Feld "Username" (Benutzername) - Geben Sie den Parameter des Benutzernamens ein, der in der URL verwendet wird. Beispielsweise *username*=admin, wobei *username* das Feld "username" (Benutzername) ist.
   f. Feld "Password" (Kennwort) - Geben Sie den Parameter des Kennworts ein, der in der URL verwendet wird. Beispielsweise *password*=raritan, wobei *password* das Feld "password " (Kennwort) ist.
10. Klicken Sie auf OK.



So ändern Sie den aktiven Status eines KVM-Switch-Ports oder einer URL:

1. Wählen Sie "Device Settings" > "Port Configuration" (Geräteeinstellungen > Portkonfiguration) aus. Die Seite "Port Configuration" (Portkonfiguration) wird angezeigt.
2. Klicken Sie auf den Portnamen des Zielservers, den Sie umbenennen möchten. Die Seite "Port" wird angezeigt.
3. Deaktivieren Sie das Kontrollkästchen "Active" (Aktiv) neben dem KVM-Switch-Zielport oder neben der URL, um den aktiven Status zu ändern.
4. Klicken Sie auf OK.

Konfiguration von Powerstrip-Zielen (Gestell-PDUs)

Mit dem KX II können Sie Powerstrips (Gestell-PDUs) mit KX II-Ports verbinden. Die KX II-Powerstrip-Konfiguration erfolgt auf der Seite "KX II Port Configuration" (KX II-Port-Konfiguration).

Verbinden von Powerstrips

Die Powerstrips der Serien Raritan PX werden über das D2CIM-PWR CIM mit dem KX II verbunden.

So schließen Sie den Powerstrip an:

1. Verbinden Sie den RJ-45-Stecker des D2CIM-PWR mit der RJ-45-Buchse des seriellen Ports des Powerstrips.
2. Verbinden Sie die RJ-45-Buchse des D2CIM-PWR mit einer der freien Systemport-Buchsen des Dominion KX II mittels eines Straight-Through-Kabels der Kategorie 5.
3. Schließen Sie ein Netzkabel am Zielserver und einem verfügbaren Powerstripausgang an.
4. Stecken Sie den Stecker des Netzkabels in eine Steckdose.

5. Schalten Sie das Gerät ein.



Benennen des Powerstrips im KX II (Seite "Port" für Powerstrips)

Hinweis: PX-Powerstrips können im PX-Gerät und im KX II benannt werden.

Diese Portseite wird angezeigt, wenn Sie auf der Seite "Port Configuration" (Portkonfiguration) einen Port auswählen, der mit einem Remotepowerstrip von Raritan verbunden ist. Die Felder "Type" (Typ) und "Name" sind bereits ausgefüllt.

Hinweis: Der (CIM-)Typ kann nicht geändert werden.

Die folgenden Informationen werden für jeden Ausgang des Powerstrips angezeigt: [Outlet] Number ([Ausgangs]nummer), Name und Port Association (Portzuordnung).

Auf dieser Seite können Sie den Powerstrip und die Ausgänge benennen. Jeder Name darf maximal 32 alphanumerische Zeichen und Sonderzeichen umfassen.

Hinweis: Wenn ein Powerstrip einem Zielserver (Port) zugeordnet ist, wird der Ausgangsname durch den Namen des Zielservers ersetzt (auch wenn Sie dem Ausgang einen anderen Namen zugeordnet haben).

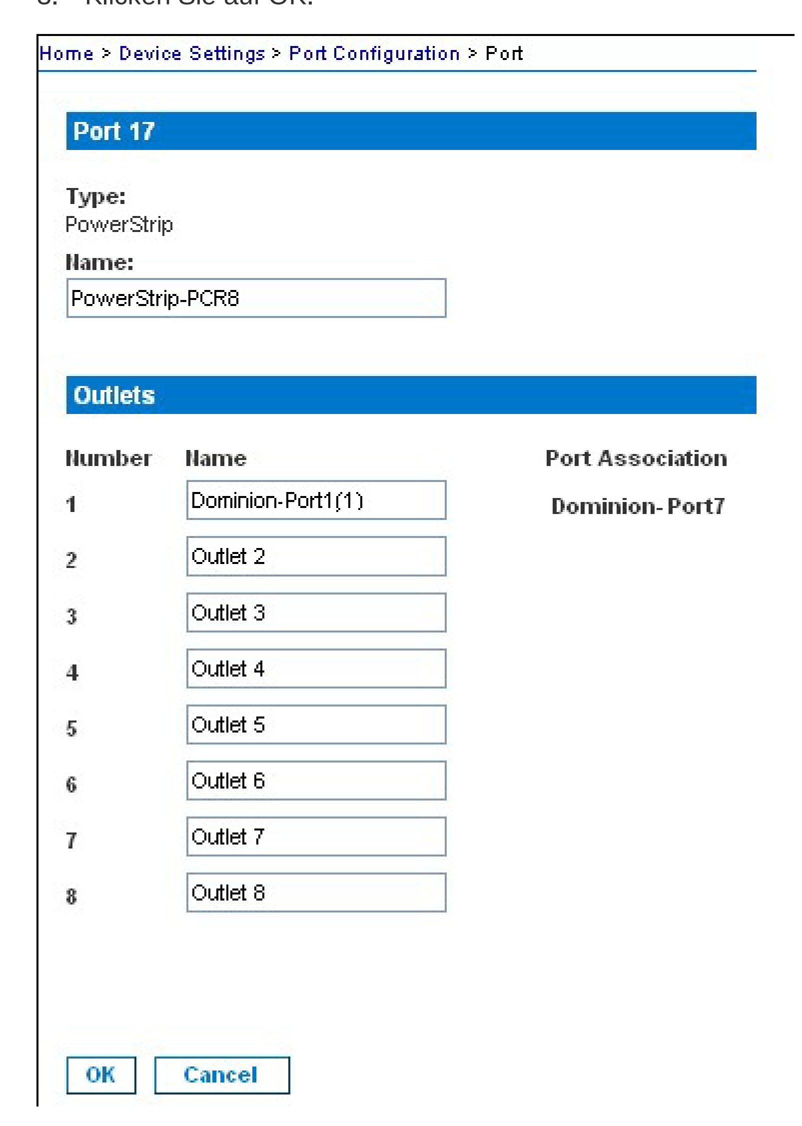
▶ So benennen Sie den Powerstrip (und seine Ausgänge):

Hinweis: Das CommandCenter-Dienstgateway erkennt Powerstripnamen mit Leerzeichen nicht.

1. Geben Sie den Namen des Powerstrip ein (falls erforderlich).
2. Ändern Sie ggf. den [Ausgangs-]namen. (Der Standardname entspricht der Ausgangsnummer.)



3. Klicken Sie auf OK.



Zuordnen von Ausgängen mit Zielservern am KX II

Die Seite "Port" wird geöffnet, wenn Sie auf der Seite "Port Configuration" (Portkonfiguration) auf einen Port klicken. Auf dieser Seite können Sie Stromzuordnungen vornehmen, den Portnamen ändern und die Einstellungen der Zielserver aktualisieren, falls Sie mit dem D2CIM-VUSB CIM arbeiten. Die Felder "(CIM)Type" [(CIM-)Typ] und "(Port) Name" [(Port-)name] enthalten bereits Werte. Beachten Sie, dass der CIM-Typ nicht geändert werden kann.

Ein Server kann maximal vier Netzschalter haben, und Sie können jedem einen anderen Powerstrip zuordnen. Auf dieser Seite können Sie diese Zuordnungen definieren, damit Sie auf der Seite "Port Access" (Portzugriff) den Server einschalten, ausschalten sowie aus- und wieder einschalten können.

Für dieses Feature benötigen Sie Folgendes:

- Remotepowerstrip(s) von Raritan
- Power CIMs (D2CIM-PWR)

So stellen Sie Stromzuordnungen her (ordnen Powerstripausgänge KVM-Zielservern zu):

Hinweis: Wenn ein Powerstrip einem Zielserver (Port) zugeordnet ist, wird der Ausgangsname durch den Namen des Zielservers ersetzt (auch wenn Sie dem Ausgang einen anderen Namen zugeordnet haben).

---

1. Wählen Sie einen Powerstrip in der Dropdownliste "Power Strip Name" (Powerstripname) aus.
2. Wählen Sie einen Ausgang für diesen Powerstrip in der Dropdownliste "Outlet Name" (Ausgangsname) aus.
3. Wiederholen Sie die Schritte 1 und 2 für alle gewünschten Stromzuordnungen.
4. Klicken Sie auf OK. Eine Bestätigungsmeldung wird angezeigt.

So ändern Sie den Portnamen:

1. Geben Sie einen aussagekräftigen Namen im Feld "Name" ein. Der Name des Zielservers wäre eine gute Wahl. Der Name darf maximal 32 alphanumerische Zeichen und Sonderzeichen umfassen.
2. Klicken Sie auf OK.



Entfernen von Stromzuordnungen

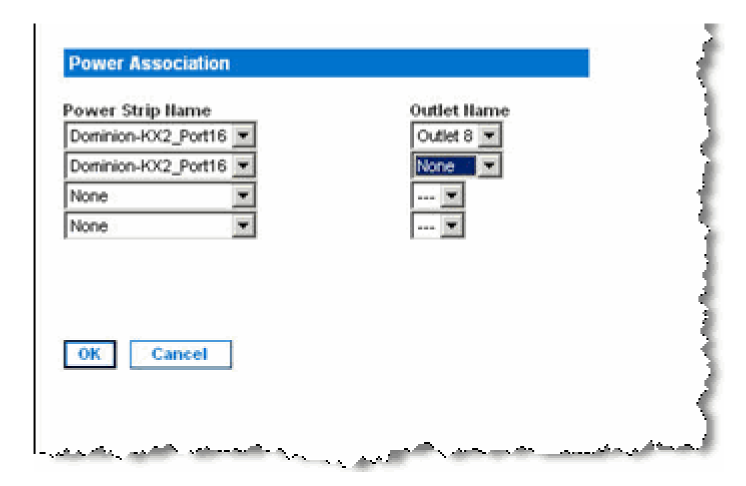
Wenn Sie Zielserver und/oder Powerstrips vom KX II trennen möchten, müssen zuvor alle Stromzuordnungen gelöscht werden. Wenn ein Zielgerät einem Powerstrip zugeordnet ist und das Zielgerät vom KX II entfernt wird, bleibt die Sromzuordnung erhalten. In diesem Fall können Sie nicht auf die Portkonfiguration des getrennten Zielservers unter "Device Settings" (Geräteeinstellungen) zugreifen, um die Stromzuordnung ordnungsgemäß zu löschen.

So entfernen Sie eine Powerstripzuordnung:

1. Wählen Sie einen Powerstrip in der Dropdownliste "Power Strip Name" (Powerstrip-Name) aus.
2. Wählen Sie einen Ausgang für diesen Powerstrip in der Dropdownliste "Outlet Name" (Ausgangsname) aus.
3. Wählen Sie in der Dropdownliste "Outlet Name" (Ausgangsname) die Option "None" (Kein).
4. Klicken Sie auf OK. Die Powerstrip-/Ausgangszuordnung wird entfernt und eine Bestätigungsmeldung wird angezeigt.

So entfernen Sie eine Powerstripzuordnung, wenn der Powerstrip vom Zielgerät entfernt wurde:

1. Klicken Sie auf "Device Settings" > "Port Configuration" (Geräteeinstellungen > Portkonfiguration) und anschließend auf das aktive Zielgerät.
2. Ordnen Sie das aktive Zielgerät dem getrennten Stromversorgungsport zu. Dadurch wird die Stromzuordnung des getrennten Zielgeräts aufgehoben.
3. Ordnen Sie anschließend das aktive Zielgerät dem richtigen Stromversorgungsport zu.



Konfigurieren von Blade-Chassis

Zusätzlich zu Standardservern und Powerstrips bietet Dominion KX II die Möglichkeit, Blade-Chassis, die an einem Dominion KX II-Port angeschlossen sind, zu steuern. Bis zu acht Blade-Chassis können gleichzeitig über Dominion KX II verwaltet werden.

Wie bei Standardservern werden auch Blade-Chassis automatisch von Dominion KX II erkannt, sobald eine Verbindung hergestellt wurde. Wenn Ein Bladeserver-Chassis von Dominion KX II erkannt wurde, wird diesem ein Standardname zugewiesen und es wird auf der Seite "Port Access" (Portzugriff) zusammen mit Standardzielservern und Powerstrips angezeigt (siehe ***Seite "Port Access" (Portzugriff)*** (auf Seite 50)). Das Blade-Chassis wird in einer erweiterbaren, hierarchischen Liste auf der Seite "Port Access" (Portzugriff) angezeigt, wobei das Blade-Chassis auf Stammebene der Hierarchie angezeigt und die einzelnen Blades unterhalb der Stammebene bezeichnet und angezeigt werden. Verwenden Sie das Symbol "Expand Arrow" (Pfeil erweitern) neben dem Stamm-Chassis, um die einzelnen Blades anzuzeigen.

Hinweis: Um das Blade-Chassis in hierarchischer Reihenfolge anzuzeigen, müssen für das Bladeserver-Chassis Blade-Chassis-Subtypen konfiguriert werden.

Mit Ausnahme von Blade-Chassis von HP® werden generische Blade-Chassis und Blade-Chassis von IBM® und Dell® auf der Seite "Port" konfiguriert. Der mit dem Blade-Chassis verbundene Port muss mit dem Blade-Chassis-Modell konfiguriert werden. Die speziellen Konfigurationsmöglichkeiten für einen Bladeserver hängen von der Marke des Bladeservers ab, den Sie verwenden. Spezielle Informationen zu allen unterstützten Blade-Chassis finden Sie in den jeweiligen Themenbereichen in diesem Abschnitt des Hilfedokuments.

Die folgenden Blade-Chassis werden unterstützt:

- IBM BladeCenter® Modelle E und H
- Dell PowerEdge® 1855, 1955 und M1000e

Eine Option für generische Blade-Chassis ermöglicht es Ihnen, ein Blade-Chassis zu konfigurieren, das nicht in der oben genannten Liste aufgeführt ist. HP BladeSystem c3000 und c7000 werden über individuelle Verbindungen zwischen Dominion KX II und dem einzelnen Blade unterstützt. Die Ports werden mithilfe des Features "Port Group Management" (Portgruppenverwaltung) in einer Chassis-Darstellung gruppiert.

Hinweis: Die Dell PowerEdge 1855/1955-Blades bieten außerdem die Möglichkeit, von jedem individuellen Blade aus eine Verbindung zu einem Port des Dominion KX II herzustellen. Wenn auf diese Weise eine Verbindung hergestellt wurde, können die Blades auch gruppiert werden und somit Bladeservergruppen bilden.



Für Blade-Chassis stehen je nach Funktionen des Blade-Chassis zwei Betriebsmodi zur Verfügung: manuelle Konfiguration und automatische Erkennung. Wenn ein Blade-Chassis für die automatische Erkennung konfiguriert wird, werden Zustandsänderungen in den folgenden Fällen von Dominion KX II nachverfolgt und aktualisiert:

- Wenn ein neuer Bladeserver zum Chassis hinzugefügt wird.
- Wenn ein bestehender Bladeserver vom Chassis entfernt wird.

Hinweis: Bei den IBM-Blade-Center-Modellen E und H unterstützt der Dominion KX II nur die automatische Erkennung für AMM[1] als aktives primäres Verwaltungsmodul.

Dominion KX II unterstützt außerdem die Verwendung von Tastenfolgen, um den KVM-Zugriff auf ein Blade-Chassis zu übertragen. Die Optionen für Blade-Chassis, bei denen Benutzer eine Tastenkombination auswählen können, sind auf der Seite "Port Configuration" (Portkonfiguration) verfügbar. Die Tastenfolgen für Blade-Chassis, bei denen diese vordefiniert sind, sind auf der Seite "Port Configuration" (Portkonfiguration) bereits in den entsprechenden Feldern eingegeben, wenn das Blade-Chassis ausgewählt wird. Wenn die Standardtastenfolge für die Übertragung des KVM-Zugriffs auf ein IBM BladeCenter H beispielsweise "NumLock + NumLock + SlotNummer" lautet, wird diese Tastenfolge standardmäßig angewendet, wenn das IBM BladeCenter H während der Konfiguration ausgewählt wird. Weitere Informationen zu den Tastenfolgen finden Sie in der Dokumentation Ihres Blade-Chassis.

Sie können die Verbindung zu einer Blade-Chassis-Webbrowseroberfläche konfigurieren, wenn verfügbar. Auf Chassis-Ebene können bis zu vier Verknüpfungen definiert werden. Die erste Verknüpfung ist für die Verbindung zur Administrativmodul-GUI für Blade-Chassis reserviert. Diese Verknüpfung kann beispielsweise vom technischen Kundendienst verwendet werden, um eine Chassis-Konfiguration schnell zu überprüfen.

Blade-Chassis können vom Dominion KX II-Virtual KVM Client (VKC), vom Multi-Platform-Client (MPC) von Raritan und von CC-SG verwaltet werden. Das Verwalten von Bladeservern über den VKC und den MPC entspricht der Verwaltung von Standard-Zielservern. Weitere Informationen finden Sie unter ***Arbeiten mit Zielservern*** (auf Seite 43) und im Administratorhandbuch **CC-SG Administrators Guide**. Alle Änderungen der Blade-Chassis-Konfiguration in Dominion KX II werden auf diese Client-Anwendungen übertragen.

Wichtig: Wenn das CIM, das das Blade-Chassis mit Dominion KX II verbindet, ausgeschaltet ist oder die Verbindung von Dominion KX II getrennt wurde, werden alle bestehenden Verbindungen zum Blade-Chassis beendet. Wenn die Verbindung über das CIM wieder hergestellt ist oder dieses eingeschaltet wurde, müssen Sie die Verbindung(en) erneut herstellen.

Wenn Sie den KX II-Port eines Blade-Chassis ändern, gehen Benutzeroberflächen, die dem Blade-Chassis-Knoten in CC-SG hinzugefügt wurden, für CC-SG verloren. Alle weiteren Informationen bleiben erhalten.

Konfigurieren von generischen Blade-Chassis

Bei Auswahl der Option "Generic Blade Chassis" (generische Blade-Chassis) steht Ihnen nur die manuelle Konfiguration zur Verfügung. Weitere wichtige Informationen zur Konfiguration von Blade-Chassis finden Sie unter ***Unterstützte Blade-Chassis-Modelle*** (auf Seite 215), ***Unterstützte CIMs für Blade-Chassis*** (auf Seite 215) und ***Erforderliche und empfohlene Blade-Chassis-Konfigurationen*** (auf Seite 219).

1. Verbinden Sie das Blade-Chassis mit Dominion KX II. Weitere Einzelheiten finden Sie unter ***Schritt 3: Anschließen der Geräte*** (siehe "***Schritt 3: Anschließen der Geräte***" auf Seite 30).
2. Wählen Sie "Device Settings" > "Port Configuration" (Geräteeinstellungen > Portkonfiguration) aus, um die Seite "Port Configuration" (Portkonfiguration) zu öffnen.
3. Klicken Sie auf der Seite "Port Configuration" (Portkonfiguration) auf den Namen des Blade-Chassis, das Sie konfigurieren möchten. Die Seite "Port" wird angezeigt.
4. Aktivieren Sie das Optionsfeld "Blade Chassis" (Blade-Chassis). Auf der Seite werden nun die für die Konfiguration eines Blade-Chassis erforderlichen Felder angezeigt.
5. Wählen Sie aus der Dropdownliste "Blade Server Chassis Model" (Bladeserver-Chassis-Modell) die Option "Generic" (Generisch) aus.
6. Konfigurieren Sie das Blade-Chassis wie gewünscht.
   a. Switch Hot Key Sequence (Tastenfolge zum Wechseln) – Definieren Sie die Tastenfolge, die Sie verwenden möchten, um vom KVM zum Blade-Chassis zu wechseln. Die Tastenfolge zum Wechseln muss der Tastenfolge entsprechen, die im Blade-Chassis vom KVM-Modul verwendet wird.
   b. Administrative Module Primary IP Address/Host Name (Administrativmodul für primäre IP-Adresse/Hostnamen) – Nicht zutreffend.
   c. Maximum Number of Slots (Maximale Anzahl an Slots) – Geben Sie die standardmäßige maximale Anzahl an Slots ein, die auf dem Blade-Chassis verfügbar sind.
   d. Port Number (Portnummer) – Die Standardportnummer für Blade-Chassis lautet 22. Nicht zutreffend.
   e. Username (Benutzername) – Nicht zutreffend.
   f. Password (Kennwort) – Nicht zutreffend.



7. Ändern Sie ggf. den Namen des Blade-Chassis.
8. Geben Sie die im Blade-Chassis installierten Blades an, indem Sie das Kontrollkästchen "Installed" (Installiert) neben allen Slots, für die ein Blade installiert ist, aktivieren. Alternativ können Sie das Kontrollkästchen "Select All" (Alle auswählen) verwenden. Ändern Sie ggf. die Bladeservernamen.
9. Im Abschnitt "Blade Chassis Managed Links" (Verwaltete Blade-Chassis-Verknüpfungen) der Seite können Sie die Verbindung zu einer Blade-Chassis-Webbrowseroberfläche konfigurieren, wenn verfügbar. Klicken Sie auf das Symbol für verwaltete Blade-Chassis-Verknüpfungen ► Blade Chassis Managed Links, um den Abschnitt auf der Seite zu erweitern.

   Die erste URL-Verknüpfung wird normalerweise für die Verbindung zur Administrativmodul-GUI für Blade-Chassis verwendet.

   Hinweis: Der Zugriff auf die URL-Verknüpfungen, die in diesem Abschnitt der Seite eingegeben wurden, wird durch die Portberechtigungen für Blade-Chassis überwacht.

   ---

   a. Active (Aktiv) – Aktivieren Sie das Kontrollkästchen "Active" (Aktiv), um die Verknüpfung nach der Konfiguration zu aktivieren. Aktiveren Sie das Kontrollkästchen nicht, wenn die Verknüpfung inaktiv bleiben soll. In die Verknüpfungsfelder können Informationen auch dann eingegeben und gespeichert werden, wenn "Active" (Aktiv) nicht ausgewählt wurde. Wenn "Active" (Aktiv) ausgewählt wurde, muss im URL-Feld eine Eingabe vorgenommen werden. Benutzername, Kennwort sowie die Felder "Username" (Benutzername) und "Password" (Kennwort) sind optional (abhängig davon, ob eine Einzelanmeldung gewünscht wird oder nicht).
   b. URL – Geben Sie die URL zur Benutzeroberfläche ein. Erforderlich
   c. Username (Benutzername) – Geben Sie den Benutzernamen ein, der für den Zugriff auf die Benutzeroberfläche verwendet wird. Optional
   d. Password (Kennwort) – Geben Sie das Kennwort ein, das für den Zugriff auf die Benutzeroberfläche verwendet wird. Optional

   ---

   Hinweis: Geben Sie bei DRAC-, ILO- und RSA-Webanwendungen keine Werte in die Felder "Username" (Benutzername) und "Password" (Kennwort) ein, da ansonsten die Verbindung fehlschlägt.



e. Die optionalen Felder "Username Field" (Benutzernamenfeld) und "Password Field" (Kennwortfeld) enthalten die Bezeichnungen, die den Einträgen für Benutzername und Kennwort zugeordnet sein sollten. In diese Felder sollten Sie die Feldnamen für die Felder "Username" (Benutzername) und "Password" (Kennwort) eingeben, die auf der Anmeldeseite der Webanwendung verwendet wurden. Sie können die HTML-Quelldatei der Anmeldeseite anzeigen, um die Feld*namen* zu suchen (nicht die Feldbezeichnungen). Tipps zum Hinzufügen einer Webbrowseroberfläche finden Sie unter ***Tipps zum Hinzufügen einer Webbrowseroberfläche*** (auf Seite 210). **Optional**

10. USB-Profilinformationen sind für eine generische Konfiguration nicht verfügbar.
11. Wählen Sie im Bereich "Target Settings" (Zieleinstellungen) die Option "720x400 Compensation" (720x400-Kompensierung) aus, wenn das Ziel diese Auflösung verwendet und Anzeigeprobleme auftreten.
12. Wählen Sie "Use international keyboard for scan code set 3" (Internationale Tastatur für Scancode Satz 3 verwenden) aus, wenn Sie mit einem DCIM-PS2 die Verbindung zum Ziel herstellen und den Scancode Satz 3 mit einer internationalen Tastatur verwenden müssen.
13. Klicken Sie zum Speichern der Konfiguration auf OK.

Konfigurieren von Dell-Blade-Chassis

Weitere wichtige Informationen zur Konfiguration von Blade-Chassis finden Sie unter ***Unterstützte Blade-Chassis-Modelle*** (auf Seite 215), ***Unterstützte CIMs für Blade-Chassis*** (auf Seite 215) und ***Erforderliche und empfohlene Blade-Chassis-Konfigurationen*** (auf Seite 219). Informationen zu Kabellänge und Videoauflösungen bei der Verwendung von Dell®-Chassis mit Dominion KX II finden Sie unter ***Kabellängen und Videoauflösungen für Dell-Chassis*** (auf Seite 347).

1. Verbinden Sie das Blade-Chassis mit Dominion KX II. Weitere Einzelheiten finden Sie unter ***Schritt 3: Anschließen der Geräte*** (siehe "***Schritt 3: Anschließen der Geräte***" auf Seite 30).
2. Wählen Sie "Device Settings" > "Port Configuration" (Geräteeinstellungen > Portkonfiguration) aus, um die Seite "Port Configuration" (Portkonfiguration) zu öffnen.
3. Klicken Sie auf der Seite "Port Configuration" (Portkonfiguration) auf den Namen des Blade-Chassis, das Sie konfigurieren möchten. Die Seite "Port" wird angezeigt.
4. Aktivieren Sie das Optionsfeld "Blade Chassis" (Blade-Chassis). Auf der Seite werden nun die für die Konfiguration eines Blade-Chassis erforderlichen Felder angezeigt.



5. Wählen Sie aus der Dropdownliste "Blade Server Chassis Model" (Bladeserver-Chassis-Modell) das Blade-Chassis-Modell von Dell aus.

So konfigurieren Sie ein Dell PowerEdge M1000e:

1. Wenn Sie das Dell PowerEdge® M1000e ausgewählt haben, ist die automatische Erkennung verfügbar. Konfigurieren Sie das Blade-Chassis wie gewünscht. Vor der Konfiguration eines Blade-Chassis, das automatisch erkannt werden kann, muss dieses so konfiguriert werden, dass SSH-Verbindungen für die festgelegte Portnummer ermöglicht werden (siehe ***Device Services (Gerätedienste)*** (auf Seite 164)). Außerdem muss zuvor auf dem Blade-Chassis ein Benutzerkonto mit den entsprechenden Authentifizierungsdaten erstellt werden.
   a. Switch Hot Key Sequence (Tastenfolge zum Wechseln) – Wählen Sie die Tastenfolge aus, die Sie verwenden möchten, um vom KVM zum Bladeserver zu wechseln. Die Tastenfolge zum Wechseln muss der Tastenfolge entsprechen, die im Blade-Chassis vom KVM-Modul verwendet wird.
   b. Maximum Number of Slots (Maximale Anzahl an Slots) – Die standardmäßige maximale Anzahl an Slots, die auf dem Blade-Chassis verfügbar sind, wird automatisch eingegeben.
   c. Administrative Module Primary IP Address/Host Name (Administrativmodul für primäre IP-Adresse/Hostnamen) – Geben Sie die primäre IP-Adresse für das Blade-Chassis ein. **Für den automatischen Erkennungsmodus erforderlich**
   d. Port Number (Portnummer) – Die Standardportnummer für Blade-Chassis lautet 22. Ändern Sie ggf. die Portnummer. **Für den automatischen Erkennungsmodus erforderlich**
   e. Username (Benutzername) – Geben Sie den Benutzernamen ein, der für den Zugriff auf das Blade-Chassis verwendet wird. **Für den automatischen Erkennungsmodus erforderlich**
   f. Password (Kennwort) – Geben Sie das Kennwort ein, das für den Zugriff auf das Blade-Chassis verwendet wird. **Für den automatischen Erkennungsmodus erforderlich**
2. Wenn Sie möchten, dass Dominion KX II Chassis-Blades automatisch erkennt, aktivieren Sie das Kontrollkästchen "Blade Auto-Discovery" (Automatische Blade-Erkennung) und klicken Sie anschließend auf die Schaltfläche "Discover Blades on Chassis Now" (Blades auf Chassis jetzt suchen). Wenn die Blades erkannt wurden, werden sie auf der Seite angezeigt.
3. Ändern Sie ggf. den Namen des Blade-Chassis. Wenn das Chassis bereits benannt wurde, erscheint der Name automatisch in diesem Feld. Wenn es noch nicht benannt wurde, wird dem Chassis von Dominion KX II ein Name zugewiesen. Die Standard-Namenskonvention für Blade-Chassis durch Dominion KX II lautet "# Blade_Chassis_Port#".

4. Wenn Sie sich im Modus "Manual" (Manuell) befinden, geben Sie die im Blade-Chassis installierten Blades an, indem Sie das Kontrollkästchen "Installed" (Installiert) neben allen Slots, für die ein Blade installiert ist, aktivieren. Alternativ können Sie das Kontrollkästchen "Select All" (Alle auswählen) verwenden. Ändern Sie ggf. die Bladeservernamen.

   Wenn Sie sich im Modus "Auto-discovery" (Automatische Erkennung) befinden, werden im Feld "Installed" (Installiert) die Slots angezeigt, die bei der Erkennung Blades enthalten.

5. Im Abschnitt "Blade Chassis Managed Links" (Verwaltete Blade-Chassis-Verknüpfungen) der Seite können Sie die Verbindung zu einer Blade-Chassis-Webbrowseroberfläche konfigurieren, wenn verfügbar. Klicken Sie auf das Symbol für verwaltete Blade-Chassis-Verknüpfungen ▸ Blade Chassis Managed Links, um den Abschnitt auf der Seite zu erweitern.

   Die erste URL-Verknüpfung wird normalerweise für die Verbindung zur Administrativmodul-GUI für Blade-Chassis verwendet.

   Hinweis: Der Zugriff auf die URL-Verknüpfungen, die in diesem Abschnitt der Seite eingegeben wurden, wird durch die Portberechtigungen für Blade-Chassis überwacht.

   ---

   a. Active (Aktiv) – Aktivieren Sie das Kontrollkästchen "Active" (Aktiv), um die Verknüpfung nach der Konfiguration zu aktivieren. Aktiveren Sie das Kontrollkästchen nicht, wenn die Verknüpfung inaktiv bleiben soll. In die Verknüpfungsfelder können Informationen auch dann eingegeben und gespeichert werden, wenn "Active" (Aktiv) nicht ausgewählt wurde. Wenn "Active" (Aktiv) ausgewählt wurde, muss im URL-Feld eine Eingabe vorgenommen werden. Benutzername, Kennwort sowie die Felder "Username" (Benutzername) und "Password" (Kennwort) sind optional (abhängig davon, ob eine Einzelanmeldung gewünscht wird oder nicht).

   b. URL – Geben Sie die URL zur Benutzeroberfläche ein. Beispielkonfigurationen für Dell M1000e finden Sie unter ***Beispiel-URL-Formate für Blade-Chassis*** (auf Seite 221).

   c. Username (Benutzername) – Geben Sie den Benutzernamen ein, der für den Zugriff auf die Benutzeroberfläche verwendet wird.

   d. Password (Kennwort) – Geben Sie das Kennwort ein, das für den Zugriff auf die Benutzeroberfläche verwendet wird.

   Hinweis: Geben Sie bei DRAC-, ILO- und RSA-Webanwendungen keine Werte in die Felder "Username" (Benutzername) und "Password" (Kennwort) ein, da ansonsten die Verbindung fehlschlägt.



e. Die optionalen Felder "Username Field" (Benutzernamenfeld) und "Password Field" (Kennwortfeld) enthalten die Bezeichnungen, die den Einträgen für Benutzername und Kennwort zugeordnet sein sollten. In diese Felder sollten Sie die Feldnamen für die Felder "Username" (Benutzername) und "Password" (Kennwort) eingeben, die auf der Anmeldeseite der Webanwendung verwendet wurden. Sie können die HTML-Quelldatei der Anmeldeseite anzeigen, um die Feld*namen* zu suchen (nicht die Feldbezeichnungen). Tipps zum Hinzufügen einer Webbrowseroberfläche finden Sie unter ***Tipps zum Hinzufügen einer Webbrowseroberfläche*** (auf Seite 210).

6. USB-Profile sind für Dell-Chassis nicht verfügbar.
7. Wählen Sie im Bereich "Target Settings" (Zieleinstellungen) die Option "720x400 Compensation" (720x400-Kompensierung) aus, wenn das Ziel diese Auflösung verwendet und Anzeigeprobleme auftreten.
8. Wählen Sie "Use international keyboard for scan code set 3" (Internationale Tastatur für Scancode Satz 3 verwenden) aus, wenn Sie mit einem DCIM-PS2 die Verbindung zum Ziel herstellen und den Scancode Satz 3 mit einer internationalen Tastatur verwenden müssen.
9. Klicken Sie zum Speichern der Konfiguration auf OK.

So konfigurieren Sie ein Dell PowerEdge 1855/1955:

1. Wenn Sie das Dell 1855/1955 ausgewählt haben, ist die automatische Erkennung *nicht verfügbar*. Konfigurieren Sie das Blade-Chassis wie gewünscht.
   a. Switch Hot Key Sequence (Tastenfolge zum Wechseln) – Wählen Sie die Tastenfolge aus, die Sie verwenden möchten, um vom KVM zum Bladeserver zu wechseln.
   b. Maximum Number of Slots (Maximale Anzahl an Slots) – Die standardmäßige maximale Anzahl an Slots, die auf dem Blade-Chassis verfügbar sind, wird automatisch eingegeben.
   c. Administrative Module Primary IP Address/Host Name (Administrativmodul für primäre IP-Adresse/Hostnamen) – Nicht zutreffend.
   d. Port Number (Portnummer) – Die Standardportnummer für Blade-Chassis lautet 22. Nicht zutreffend.
   e. Username (Benutzername) – Nicht zutreffend.
   f. Password (Kennwort) – Nicht zutreffend.
2. Ändern Sie ggf. den Namen des Blade-Chassis.

3. Geben Sie die im Blade-Chassis installierten Blades an, indem Sie das Kontrollkästchen "Installed" (Installiert) neben allen Slots, für die ein Blade installiert ist, aktivieren. Alternativ können Sie das Kontrollkästchen "Select All" (Alle auswählen) verwenden. Ändern Sie ggf. die Bladeservernamen.
4. Im Abschnitt "Blade Chassis Managed Links" (Verwaltete Blade-Chassis-Verknüpfungen) der Seite können Sie die Verbindung zu einer Blade-Chassis-Webbrowseroberfläche konfigurieren, wenn verfügbar. Klicken Sie auf das Symbol für verwaltete Blade-Chassis-Verknüpfungen ► Blade Chassis Managed Links, um den Abschnitt auf der Seite zu erweitern.

   Die erste URL-Verknüpfung wird normalerweise für die Verbindung zur Administrativmodul-GUI für Blade-Chassis verwendet.

   Hinweis: Der Zugriff auf die URL-Verknüpfungen, die in diesem Abschnitt der Seite eingegeben wurden, wird durch die Portberechtigungen für Blade-Chassis überwacht.

   ---

   a. Active (Aktiv) – Aktivieren Sie das Kontrollkästchen "Active" (Aktiv), um die Verknüpfung nach der Konfiguration zu aktivieren. Aktiveren Sie das Kontrollkästchen nicht, wenn die Verknüpfung inaktiv bleiben soll. In die Verknüpfungsfelder können Informationen auch dann eingegeben und gespeichert werden, wenn "Active" (Aktiv) nicht ausgewählt wurde. Wenn "Active" (Aktiv) ausgewählt wurde, muss im URL-Feld eine Eingabe vorgenommen werden. Benutzername, Kennwort sowie die Felder "Username" (Benutzername) und "Password" (Kennwort) sind optional (abhängig davon, ob eine Einzelanmeldung gewünscht wird oder nicht).
   b. URL – Geben Sie die URL zur Benutzeroberfläche ein. Beispielkonfigurationen für Dell PowerEdge 1855/1955 finden Sie unter ***Beispiel-URL-Formate für Blade-Chassis*** (auf Seite 221).
   c. Username (Benutzername) – Geben Sie den Benutzernamen ein, der für den Zugriff auf die Benutzeroberfläche verwendet wird.
   d. Password (Kennwort) – Geben Sie das Kennwort ein, das für den Zugriff auf die Benutzeroberfläche verwendet wird.

   Hinweis: Geben Sie bei DRAC-, ILO- und RSA-Webanwendungen keine Werte in die Felder "Username" (Benutzername) und "Password" (Kennwort) ein, da ansonsten die Verbindung fehlschlägt.



e. Die optionalen Felder "Username Field" (Benutzernamenfeld) und "Password Field" (Kennwortfeld) enthalten die Bezeichnungen, die den Einträgen für Benutzername und Kennwort zugeordnet sein sollten. In diese Felder sollten Sie die Feldnamen für die Felder "Username" (Benutzername) und "Password" (Kennwort) eingeben, die auf der Anmeldeseite der Webanwendung verwendet wurden. Sie können die HTML-Quelldatei der Anmeldeseite anzeigen, um die Feld*namen* zu suchen (nicht die Feldbezeichnungen). Tipps zum Hinzufügen einer Webbrowseroberfläche finden Sie unter ***Tipps zum Hinzufügen einer Webbrowseroberfläche*** (auf Seite 210).

5. USB-Profile sind für Dell-Chassis nicht verfügbar.
6. Klicken Sie zum Speichern der Konfiguration auf OK.

Konfigurieren von IBM-Blade-Chassis

Weitere wichtige Informationen zur Konfiguration von Blade-Chassis finden Sie unter ***Unterstützte Blade-Chassis-Modelle*** (auf Seite 215), ***Unterstützte CIMs für Blade-Chassis*** (auf Seite 215) und ***Erforderliche und empfohlene Blade-Chassis-Konfigurationen*** (auf Seite 219).

1. Verbinden Sie das Blade-Chassis mit Dominion KX II. Weitere Einzelheiten finden Sie unter ***Schritt 3: Anschließen der Geräte*** (siehe "***Schritt 3: Anschließen der Geräte***" auf Seite 30).
2. Wählen Sie "Device Settings" > "Port Configuration" (Geräteeinstellungen > Portkonfiguration) aus, um die Seite "Port Configuration" (Portkonfiguration) zu öffnen.
3. Klicken Sie auf der Seite "Port Configuration" (Portkonfiguration) auf den Namen des Blade-Chassis, das Sie konfigurieren möchten. Die Seite "Port" wird angezeigt.
4. Aktivieren Sie das Optionsfeld "Blade Chassis" (Blade-Chassis). Auf der Seite werden nun die für die Konfiguration eines Blade-Chassis erforderlichen Felder angezeigt.
5. Wählen Sie aus der Dropdownliste "Blade Server Chassis Model" (Bladeserver-Chassis-Modell) das Blade-Chassis-Modell von IBM® aus.

So konfigurieren Sie ein IBM BladeCenter H oder E:

1. Wenn Sie das IBM BladeCenter® H oder E ausgewählt haben, ist die automatische Erkennung verfügbar. Konfigurieren Sie das Blade-Chassis wie gewünscht. Vor der Konfiguration eines Blade-Chassis, das automatisch erkannt werden kann, muss dieses so konfiguriert werden, dass SSH-Verbindungen für die festgelegte Portnummer ermöglicht werden (siehe ***Device Services (Gerätedienste)*** (auf Seite 164)). Außerdem muss zuvor auf dem Blade-Chassis ein Benutzerkonto mit den entsprechenden Authentifizierungsdaten erstellt werden. Dominion KX II unterstützt nur die automatische Erkennung für AMM[1].
   a. Switch Hot Key Sequence (Tastenfolge zum Wechseln) – Vordefiniert
   b. Maximum Number of Slots (Maximale Anzahl an Slots) – Die standardmäßige maximale Anzahl an Slots, die auf dem Blade-Chassis verfügbar sind, wird automatisch eingegeben.
   c. Administrative Module Primary IP Address/Host Name (Administrativmodul für primäre IP-Adresse/Hostnamen) – Geben Sie die primäre IP-Adresse für das Blade-Chassis ein. **Für den automatischen Erkennungsmodus erforderlich**
   d. Port Number (Portnummer) – Die Standardportnummer für Blade-Chassis lautet 22. Ändern Sie ggf. die Portnummer. **Für den automatischen Erkennungsmodus erforderlich**
   e. Username (Benutzername) – Geben Sie den Benutzernamen ein, der für den Zugriff auf das Blade-Chassis verwendet wird. **Für den automatischen Erkennungsmodus erforderlich**
   f. Password (Kennwort) – Geben Sie das Kennwort ein, das für den Zugriff auf das Blade-Chassis verwendet wird. **Für den automatischen Erkennungsmodus erforderlich**
2. Wenn Sie möchten, dass Dominion KX II Chassis-Blades automatisch erkennt, aktivieren Sie das Kontrollkästchen "Blade Auto-Discovery" (Automatische Blade-Erkennung) und klicken Sie anschließend auf die Schaltfläche "Discover Blades on Chassis Now" (Blades auf Chassis jetzt suchen). Wenn die Blades erkannt wurden, werden sie auf der Seite angezeigt.
3. Ändern Sie ggf. den Namen des Blade-Chassis. Wenn das Chassis bereits benannt wurde, erscheint der Name automatisch in diesem Feld. Wenn es noch nicht benannt wurde, wird dem Chassis von Dominion KX II ein Name zugewiesen. Die Standard-Namenskonvention für Blade-Chassis durch Dominion KX II lautet "# Blade_Chassis_Port#".



4. Wenn Sie sich im Modus "Manual" (Manuell) befinden, geben Sie die im Blade-Chassis installierten Blades an, indem Sie das Kontrollkästchen "Installed" (Installiert) neben allen Slots, für die ein Blade installiert ist, aktivieren. Alternativ können Sie das Kontrollkästchen "Select All" (Alle auswählen) verwenden. Ändern Sie ggf. die Bladeservernamen.

   Wenn Sie sich im Modus "Auto-discovery" (Automatische Erkennung) befinden, werden im Feld "Installed" (Installiert) die Slots angezeigt, die bei der Erkennung Blades enthalten.

5. Im Abschnitt "Blade Chassis Managed Links" (Verwaltete Blade-Chassis-Verknüpfungen) der Seite können Sie die Verbindung zu einer Blade-Chassis-Webbrowseroberfläche konfigurieren, wenn verfügbar. Klicken Sie auf das Symbol für verwaltete Blade-Chassis-Verknüpfungen ▸ Blade Chassis Managed Links, um den Abschnitt auf der Seite zu erweitern.

   Die erste URL-Verknüpfung wird normalerweise für die Verbindung zur Administrativmodul-GUI für Blade-Chassis verwendet.

   Hinweis: Der Zugriff auf die URL-Verknüpfungen, die in diesem Abschnitt der Seite eingegeben wurden, wird durch die Portberechtigungen für Blade-Chassis überwacht.

   a. Active (Aktiv) – Aktivieren Sie das Kontrollkästchen "Active" (Aktiv), um die Verknüpfung nach der Konfiguration zu aktivieren. Aktiveren Sie das Kontrollkästchen nicht, wenn die Verknüpfung inaktiv bleiben soll. In die Verknüpfungsfelder können Informationen auch dann eingegeben und gespeichert werden, wenn "Active" (Aktiv) nicht ausgewählt wurde. Wenn "Active" (Aktiv) ausgewählt wurde, muss im URL-Feld eine Eingabe vorgenommen werden. Benutzername, Kennwort sowie die Felder "Username" (Benutzername) und "Password" (Kennwort) sind optional (abhängig davon, ob eine Einzelanmeldung gewünscht wird oder nicht).

   b. URL – Geben Sie die URL zur Benutzeroberfläche ein. Beispielkonfigurationen für IBM BladeCenter finden Sie unter ***Beispiel-URL-Formate für Blade-Chassis*** (auf Seite 221).

   c. Username (Benutzername) – Geben Sie den Benutzernamen ein, der für den Zugriff auf die Benutzeroberfläche verwendet wird.

   d. Password (Kennwort) – Geben Sie das Kennwort ein, das für den Zugriff auf die Benutzeroberfläche verwendet wird.

   Hinweis: Geben Sie bei DRAC-, ILO- und RSA-Webanwendungen keine Werte in die Felder "Username" (Benutzername) und "Password" (Kennwort) ein, da ansonsten die Verbindung fehlschlägt.

e. Die optionalen Felder "Username Field" (Benutzernamenfeld) und "Password Field" (Kennwortfeld) enthalten die Bezeichnungen, die den Einträgen für Benutzername und Kennwort zugeordnet sein sollten. In diese Felder sollten Sie die Feldnamen für die Felder "Username" (Benutzername) und "Password" (Kennwort) eingeben, die auf der Anmeldeseite der Webanwendung verwendet wurden. Sie können die HTML-Quelldatei der Anmeldeseite anzeigen, um die Feld*namen* zu suchen (nicht die Feldbezeichnungen). Tipps zum Hinzufügen einer Webbrowseroberfläche finden Sie unter ***Tipps zum Hinzufügen einer Webbrowseroberfläche*** (auf Seite 210).

6. Definieren Sie ggf. das USB-Profil für das Blade-Chassis oder wählen Sie ein bestehendes USB-Profil aus. Klicken Sie auf das Symbol zum Auswählen des USB-Profils für einen Port **► Select USB Profiles for Port** oder das Symbol zum Übernehmen von ausgewählten Profilen für sonstige Ports **► Apply Selected Profiles to Other Ports**, um die entsprechenden Abschnitte der Seite zu erweitern. Siehe ***Konfigurieren von USB-Profilen (Seite "Port")*** (auf Seite 222).
7. Klicken Sie zum Speichern der Konfiguration auf OK.

► So konfigurieren Sie ein IBM BladeCenter (Sonstige):

1. Wenn Sie "IBM BladeCenter (Other)" [IBM BladeCenter (Sonstige)] ausgewählt haben, ist die automatische Erkennung *nicht* verfügbar. Konfigurieren Sie das Blade-Chassis wie gewünscht.
   a. Switch Hot Key Sequence (Tastenfolge zum Wechseln) – Wählen Sie die Tastenfolge aus, die Sie verwenden möchten, um vom KVM zum Bladeserver zu wechseln.
   b. Administrative Module Primary IP Address/Host Name (Administrativmodul für primäre IP-Adresse/Hostnamen) – Geben Sie die primäre IP-Adresse für das Blade-Chassis ein.Nicht zutreffend.
   c. Maximum Number of Slots (Maximale Anzahl an Slots) – Geben Sie die standardmäßige maximale Anzahl an Slots ein, die auf dem Blade-Chassis verfügbar sind.
   d. Port Number (Portnummer) – Die Standardportnummer für Blade-Chassis lautet 22. Nicht zutreffend.
   e. Username (Benutzername) – Nicht zutreffend.
   f. Password (Kennwort) – Nicht zutreffend.
2. Ändern Sie ggf. den Namen des Blade-Chassis.



3. Geben Sie die im Blade-Chassis installierten Blades an, indem Sie das Kontrollkästchen "Installed" (Installiert) neben allen Slots, für die ein Blade installiert ist, aktivieren. Alternativ können Sie das Kontrollkästchen "Select All" (Alle auswählen) verwenden. Ändern Sie ggf. die Bladeservernamen. Wenn er noch nicht benannt wurde, wird dem Bladeserver von Dominion KX II ein Name zugewiesen. Die Standard-Namenskonvention für Bladeserver lautet "# Blade_Chassis_Port#_Slot#".
4. Im Abschnitt "Blade Chassis Managed Links" (Verwaltete Blade-Chassis-Verknüpfungen) der Seite können Sie die Verbindung zu einer Blade-Chassis-Webbrowseroberfläche konfigurieren, wenn verfügbar. Klicken Sie auf das Symbol für verwaltete Blade-Chassis-Verknüpfungen ► Blade Chassis Managed Links, um den Abschnitt auf der Seite zu erweitern.

   Die erste URL-Verknüpfung wird normalerweise für die Verbindung zur Administrativmodul-GUI für Blade-Chassis verwendet.

   Hinweis: Der Zugriff auf die URL-Verknüpfungen, die in diesem Abschnitt der Seite eingegeben wurden, wird durch die Portberechtigungen für Blade-Chassis überwacht.

   ---

   a. Active (Aktiv) – Aktivieren Sie das Kontrollkästchen "Active" (Aktiv), um die Verknüpfung nach der Konfiguration zu aktivieren. Aktiveren Sie das Kontrollkästchen nicht, wenn die Verknüpfung inaktiv bleiben soll. In die Verknüpfungsfelder können Informationen auch dann eingegeben und gespeichert werden, wenn "Active" (Aktiv) nicht ausgewählt wurde. Wenn "Active" (Aktiv) ausgewählt wurde, muss im URL-Feld eine Eingabe vorgenommen werden. Benutzername, Kennwort sowie die Felder "Username" (Benutzername) und "Password" (Kennwort) sind optional (abhängig davon, ob eine Einzelanmeldung gewünscht wird oder nicht).
   b. URL – Geben Sie die URL zur Benutzeroberfläche ein. Beispielkonfigurationen für IBM BladeCenter finden Sie unter ***Beispiel-URL-Formate für Blade-Chassis*** (auf Seite 221).
   c. Username (Benutzername) – Geben Sie den Benutzernamen ein, der für den Zugriff auf die Benutzeroberfläche verwendet wird.
   d. Password (Kennwort) – Geben Sie das Kennwort ein, das für den Zugriff auf die Benutzeroberfläche verwendet wird.

   Hinweis: Geben Sie bei DRAC-, ILO- und RSA-Webanwendungen keine Werte in die Felder "Username" (Benutzername) und "Password" (Kennwort) ein, da ansonsten die Verbindung fehlschlägt.



e. Die optionalen Felder "Username Field" (Benutzernamenfeld) und "Password Field" (Kennwortfeld) enthalten die Bezeichnungen, die den Einträgen für Benutzername und Kennwort zugeordnet sein sollten. In diese Felder sollten Sie die Feldnamen für die Felder "Username" (Benutzername) und "Password" (Kennwort) eingeben, die auf der Anmeldeseite der Webanwendung verwendet wurden. Sie können die HTML-Quelldatei der Anmeldeseite anzeigen, um die Feld*namen* zu suchen (nicht die Feldbezeichnungen). Tipps zum Hinzufügen einer Webbrowseroberfläche finden Sie unter ***Tipps zum Hinzufügen einer Webbrowseroberfläche*** (auf Seite 210).

5. USB-Profile werden für Konfigurationen von IBM (Sonstige) nicht verwendet.
6. Wählen Sie im Bereich "Target Settings" (Zieleinstellungen) die Option "720x400 Compensation" (720x400-Kompensierung) aus, wenn das Ziel diese Auflösung verwendet und Anzeigeprobleme auftreten.
7. Wählen Sie "Use international keyboard for scan code set 3" (Internationale Tastatur für Scancode Satz 3 verwenden) aus, wenn Sie mit einem DCIM-PS2 die Verbindung zum Ziel herstellen und den Scancode Satz 3 mit einer internationalen Tastatur verwenden müssen.
8. Klicken Sie zum Speichern der Konfiguration auf OK.

Tipps zum Hinzufügen einer Webbrowseroberfläche

Sie können eine Webbrowseroberfläche hinzufügen, um eine Verbindung zu einem Gerät mit einem eingebetteten Webserver herzustellen. Eine Webbrowseroberfäche kann außerdem verwendet werden, um eine Verbindung mit einer beliebigen Webanwendung herzustellen (z. B. die Webanwendung, die einer RSA-, DRAC- oder ILO-Prozessorkarte zugeordnet ist).

Dazu müssen Sie DNS konfigurieren, ansonsten werden URLs nicht umgewandelt. Für IP-Adressen müssen Sie DNS nicht konfigurieren.

► So fügen Sie eine Webbrowseroberfläche hinzu:

1. Der Standardname für eine Webbrowseroberfläche wird bereitgestellt. Ändern Sie den Namen ggf. im Feld "Name".
2. Geben Sie die URL oder den Domainnamen der Webanwendung in das URL-Feld ein. Sie müssen die URL eingeben, bei der die Webanwendung normalerweise den Benutzernamen und das Kennwort ablesen kann.

   Folgen Sie unten angegebenen Beispielen, um korrekte Formate zu erhalten:

   - http(s)://192.168.1.1/login.asp



- http(s)://www.example.com/cgi/login
- http(s)://example.com/home.html

3. Geben Sie den Benutzernamen und das Kennwort ein, mit denen Sie auf diese Benutzeroberfläche zugreifen können. **Optional**
4. Wenn Sie den Benutzernamen und das Kennwort eingegebne haben, geben Sie in die Felder "Username Field" (Benutzernamenfeld) und "Password Field" (Kennwortfeld) die Feldnamen für die Felder "Username" (Benutzername) und "Password" (Kennwort) ein, die auf der Anmeldeseite der Webanwendung verwendet werden. Sie müssen die HTML-Quelldatei der Anmeldeseite anzeigen, um die Feldnamen zu suchen (nicht die Feldbezeichnungen).

Tipp zum Suchen von Feldnamen:

- Suchen Sie im HTML-Quellcode der Anmeldeseite der Webanwendung nach der Bezeichnung des Feldes [z. B. "Username" (Benutzername) oder "Password" (Kennwort)].
- Wenn Sie die Feldbezeichnung gefunden haben, suchen Sie im nebenstehenden Code nach einem Tag, der folgendermaßen aussieht: name="user". Das Wort in Anführungszeichen ist der Feldname.

Konfigurieren von HP-Blade-Chassis (Portgruppenverwaltung)

Dominion KX II unterstützt den Zusammenschluss von Ports, die mit verschiedenen Bladetypen verbunden sind, zu einer Gruppe, die das Blade-Chassis repräsentiert. Speziell HP®-BladeServer-Blades und Dell® PowerEdge® 1855/1955-Blades, wenn das DellPowerEdge 1855/1955 von jedem individuellen Blade aus mit einem Port auf Dominion KX II verbunden ist.

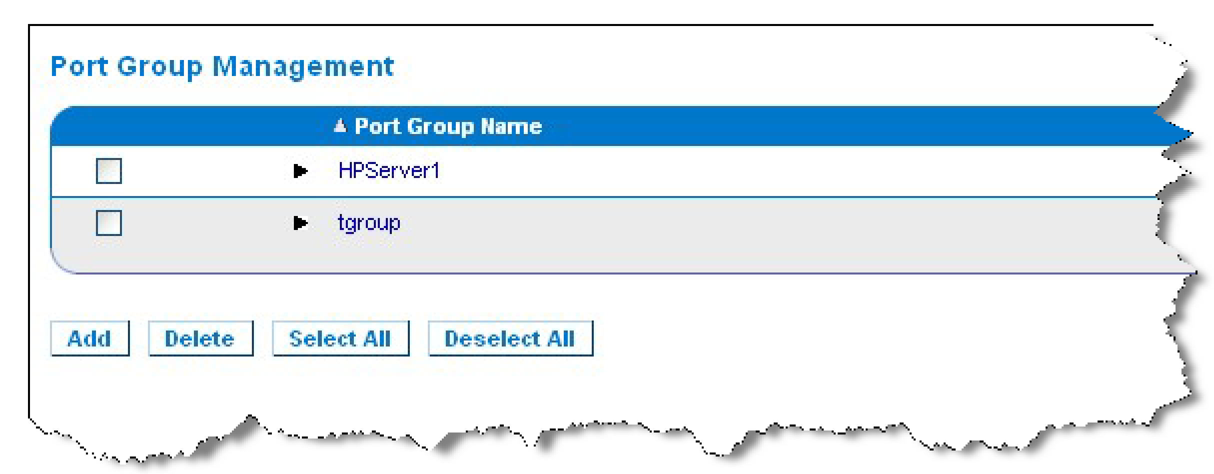
Das Chassis wird durch einen Portgruppennamen identifiziert, und die Gruppe wird als Bladeservergruppe auf der Seite "Port Group Management" (Portgruppenverwaltung) festgelegt. Portgruppen bestehen nur aus Ports, die als Standard-KVM-Ports konfiguriert wurden, nicht aus Ports, die als Blade-Chassis konfiguriert wurden. Ein Port kann nur einer einzigen Gruppe angehören.

Ports, die mit integrierten KVM-Modulen in einem Blade-Chassis verbunden sind, werden als Blade-Chassis-Untertypen konfiguriert. Diese Ports können in Portgruppen aufgenommen werden.

Wenn Dominion KX II-Ports mit integrierten KVM-Modulen in einem Blade-Chassis, nicht mit einzelnen Blades, verbunden, werden die Ports als Blade-Chassis-Untertypen konfiguriert. Diese Ports können nicht in Portgruppen aufgenommen werden und werden nicht in der Liste "Select Port for Group, Available" (Port für Gruppe auswählen, Verfügbar) angezeigt.

Wenn ein Standard-KVM-Port in eine Portgruppe aufgenommen wurde und somit im Folgenden als Blade-Chassis-Subtyp verwendet wird, muss dieser Port zunächst aus der Portgruppe entfernt werden.

Portgruppen werden mithilfe der Option "Backup and Restore" (Sicherung und Wiederherstellung) wiederhergestellt (siehe ***Backup and Restore (Sicherung und Wiederherstellung)*** (auf Seite 253)).





So fügen Sie eine Portgruppe hinzu:

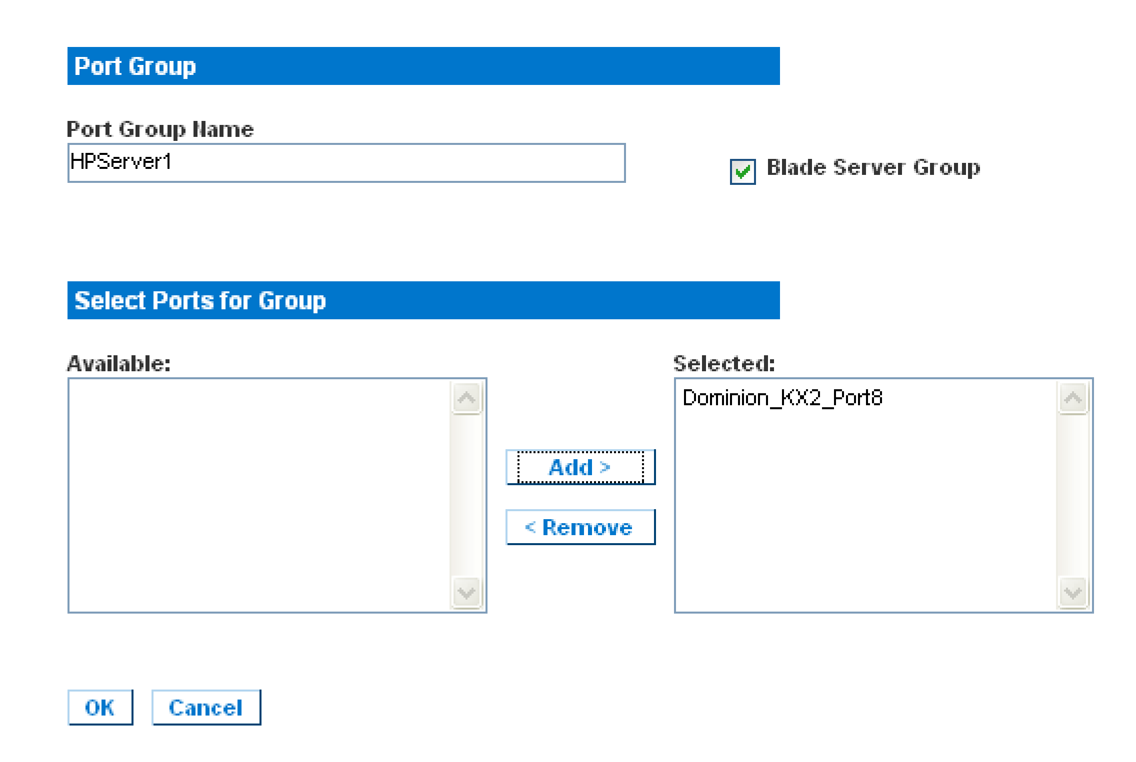
1. Klicken Sie auf "Device Settings" > "Port Group Management" (Geräteeinstellungen > Portgruppenverwaltung), um die Seite "Port Group Management" (Portgruppenverwaltung) zu öffnen.
2. Klicken Sie auf die Schaltfläche "Add" (Hinzufügen), um die Seite "Port Group" (Portgruppe) zu öffnen.
3. Geben Sie unter "Port Group Name" (Portgruppenname) einen Portgruppennamen ein. Dabei müssen Sie die Groß-/Kleinschreibung nicht beachten. Der Portgruppenname kann bis zu 32 Zeichen umfassen.
4. Aktivieren Sie das Kontrollkästchen "Blade Server Group" (Bladeservergruppe).

   Wenn Sie festlegen möchten, dass diese Ports zu Blades in einem Blade-Chassis zugeordnet werden (z. B. HP c3000 oder Dell PowerEdge 1855), aktivieren Sie das Kontrollkästchen "Blade Server Group" (Bladeservergruppe).

   Hinweis: Dies ist besonders wichtig für CC-SG-Benutzer, die HP-Blades auf Chassis-Basis organisieren möchten; jedes Blade verfügt jedoch über eine eigene Verbindung zu einem Port auf Dominion KX II.

5. Klicken Sie im Abschnitt "Select Ports for Group" (Port für Gruppe auswählen) im Feld "Available" (Verfügbar) auf einen Port. Klicken Sie auf "Add" (Hinzufügen), um den Port zur Gruppe hinzuzufügen. Der Port wird in das Feld "Selected" (Ausgewählt) verschoben.

6. Klicken Sie auf OK, um die Portgruppe hinzuzufügen.



So bearbeiten Sie Portgruppeninformationen:

1. Klicken Sie auf der Seite "Port Group Management" (Portgruppenverwaltung) auf die Verknüpfung der Portgruppe, die Sie bearbeiten möchten. Die Seite "Port Group" (Portgruppe) wird angezeigt.
2. Bearbeiten Sie die Informationen wie gewünscht.
3. Klicken Sie zum Speichern der Änderungen auf OK.

So löschen Sie eine Portgruppe:

1. Klicken Sie auf die Seite "Port Group Management" (Portgruppenverwaltung) und aktivieren Sie das Kontrollkästchen der Portgruppe, die Sie löschen möchten.
2. Klicken Sie auf die Schaltfläche "Delete" (Löschen).
3. Bestätigen Sie die Warnungsmeldung mit OK.



Unterstützte Blade-Chassis-Modelle

Die Tabelle enthält die Blade-Chassis-Modelle, die von Dominion KX II unterstützt werden, sowie die entsprechenden Profile, die pro Chassis-Modell ausgewählt werden sollten, wenn sie in der Dominion KX II-Anwendung konfiguriert werden. Eine Liste dieser Modelle kann auf der Seite "Port Configuration"(Portkonfiguration) in der Dropdownliste "Blade Server Chassis Model" (Bladeserver-Chassis-Modell) ausgewählt werden. Diese Liste wird angezeigt, wenn das Optionsfeld "Blade Chassis" (Blade-Chassis) ausgewählt wurde. Weitere Informationen zur Konfiguration der einzelnen Blade-Chassis-Modelle finden Sie in den jeweiligen Themenbereichen in diesem Abschnitt des Hilfedokuments.

Blade-Chassis-Modell	Dominion KX II-Profil
Dell® PowerEdge® 1855/1955	Dell PowerEdge 1855/1955
Dell PowerEdge M1000e	Dell PowerEdge M1000e
IBM® BladeCenter® S	IBM (Other)
IBM BladeCenter H	IBM BladeCenter H
IBM BladeCenter T	IBM (Other)
IBM BladeCenter HT	IBM (Other)
IBM BladeCenter E	IBM BladeCenter E
HP®	Konfiguration mithilfe der Funktionen der Portgruppenverwaltung Siehe ***Konfigurieren von HP-Blade-Chassis (Portgruppenverwaltung)*** (auf Seite 212).

Unterstützte CIMs für Blade-Chassis

Die folgenden CIMs werden für Blade-Chassis, die über Dominion KX II verwaltet werden, unterstützt:

- DCIM-PS2
- DCIM-USBG2
- D2CIM-VUSB
- D2CIM-DVUSB

Die folgende Tabelle enthält unterstützte CIMs für alle Blade-Chassis-Modelle, die von Dominion KX II unterstützt werden.

Blade-Chassis	Verbindungsmethode	Empfohlene(s) CIM(s)
Generisch	Wenn bei der Verbindungsherstellung zu	• DCIM-PS2

<table>
<tr><th>Blade-Chassis</th><th>Verbindungsmethode</th><th>Empfohlene(s) CIM(s)</th></tr>
<tr><td></td><td>einem als generisch konfigurierten Blade-Chassis ein D2CIM-VUSB oder D2CIM-DVUSB verwendet wird, können Sie die USB-Profile von der Seite "Port Configuration" (Portkonfiguration) und dem USB-Profilmenü des Client auswählen. Virtuelle Medien werden jedoch für generische Blade-Chassis nicht unterstützt, und das Menü "Virtual Media" (Virtuelle Medien) ist im Client deaktiviert.</td><td>DCIM-USBG2</td></tr>
<tr><td>Dell® PowerEdge® 1855</td><td>Beinhaltet eines der drei KVM-Module:
Analog KVM Ethernet switch module (Analoges KVM-Ethernet-Switchmodul) – Standard
Digital Access KVM switch module (KVM-Switchmodul für digitalen Zugriff) – Optional
KVM switch module (KVM-Switchmodul) – Standard auf Systemen, die vor April 2005 verkauft wurden
Diese Switches bieten einen benutzerdefinierten Anschluss, mit dem Sie zwei PS/2 und ein Grafikgerät am System anschließen können.

Quelle: Benutzerhandbuch Dell Poweredge 1855</td><td>DCIM-PS2</td></tr>
<tr><td>Dell PowerEdge 1955</td><td>Einer dieser beiden KVM-Modultypen kann installiert werden:
Analog KVM switch module (Analoges KVM-Switchmodul)
Digital Access KVM switch module (KVM-Switchmodul für digitalen Zugriff)
Beide Module ermöglichen es Ihnen, ein(e) PS/2-kompatible Tastatur, Maus und Videomonitor am System anzuschließen (mithilfe eines benutzerdefinierten Kabels, das mit dem System bereitgestellt wird).

Quelle: Betriebsanleitung Dell Poweredge 1955</td><td>DCIM-PS2</td></tr>
<tr><td>Dell PowerEdge M1000e</td><td>Das KVM-Switchmodul (iKVM) ist in diesem Chassis integriert.

Das iKVM ist kompatibel mit folgenden</td><td>DCIM-USBG2</td></tr>
</table>



Blade-Chassis	Verbindungsmethode	Empfohlene(s) CIM(s)
	Peripheriegeräten: • USB-Tastaturen, USB-Zeigegeräte • VGA-Monitore mit DDC-Unterstützung Quelle: *Dell Chassis Management Controller, Firmware Version 1.0, User Guide (Benutzerhandbuch Dell Chassis Management Controller, Firmware-Version 1.0)*	
HP® BladeSystem c3000	Mit dem c-Class Blade SUV-Kabel von HP können Sie die Verfahren zur Verwaltung, Konfiguration und Diagnose von Blade-Chassis durchführen, indem Sie Grafik- und USB-Geräte direkt mit dem Serverblade verbinden. Quelle: *HP Proliant™ BL480c Server Blade Maintenance and Service Guide (Instandhaltungs- und Servicehandbuch HP Proliant BL480c-Serverblade)*	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB (für Standard-KVM-Port betrieb ohne KVM-Option)
HP BladeSystem c7000	Mit dem c-Class Blade SUV-Kabel von HP können Sie die Verfahren zur Verwaltung, Konfiguration und Diagnose von Serverblades durchführen, indem Sie Grafik- und USB-Geräte direkt mit dem Serverblade verbinden. Quelle: *HP ProLiant BL480c Server Blade Maintenance and Service Guide (Instandhaltungs- und Servicehandbuch HP ProLiant BL480c-Serverblade)*	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB (für Standard-KVM-Port betrieb)
IBM® BladeCenter® S	Das Advanced Management Module (AMM) bietet Systemverwaltungsfunktionen und (KVM-)Multiplexverfahren (Tastatur/Video/Maus) für alle Blade-Chassis. Zu den AMM-Anschlüssen zählen: serieller Port, Videoverbindung, Remoteverwaltungsport (Ethernet) sowie zwei USB v2.0-Ports für Tastatur und Maus Quelle: *Implementing the IBM BladeCenter S Chassis (Implementierungsanleitung IBM BladeCenter S Chassis)*	• DCIM-USBG2
IBM BladeCenter H	Im Lieferumfang des BladeCenter H-Chassis ist standardmäßig ein Advanced Management Module enthalten. Quelle: *IBM BladeCenter Products and Technology (IBM BladeCenter-Produkte und*	• DCIM-USBG2 • D2CIM-DVUSB



Blade-Chassis	Verbindungsmethode	Empfohlene(s) CIM(s)
	-Technologie)	
IBM BladeCenter E	Im Lieferumfang des aktuellen Chassis-Modells "BladeCenter E" (8677-3Rx) ist standardmäßig ein Advanced Management Module enthalten. Quelle: *IBM BladeCenter Products and Technology (IBM BladeCenter-Produkte und -Technologie)*	• DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter T	Im Lieferumfang des BladeCenter T-Chassis ist standardmäßig ein Advanced Management Module enthalten. Im Gegensatz zum Standard-BladeCenter-Chassis bestehen das KVM-Modul und das Management Module im BladeCenter T-Chassis aus separaten Komponenten. Auf der Vorderseite des Verwaltungsmoduls sind nur die LEDs zur Anzeige des Status vorhanden. Alle Ethernet- und KVM-Verbindungen werden von der Rückseite aus mit den LAN- und KVM-Modulen verbunden. Das KVM-Modul ist ein Hot-Swap-Modul auf der Rückseite des Chassis und verfügt über zwei PS/2-Anschlüsse für Tastatur und Maus, ein Systemstatuspanel sowie einen HD-15-Videoanschluss. Quelle: *IBM BladeCenter Products and Technology (IBM BladeCenter-Produkte und -Technologie)*	• DCIM-PS2
IBM BladeCenter HT	Im Lieferumfang des BladeCenter HT-Chassis ist standardmäßig ein Advanced Management Module enthalten. Mit diesem Modul können Sie das Chassis verwalten sowie die lokale KVM-Funktion übernehmen. Quelle: *IBM BladeCenter Products and Technology (IBM BladeCenter-Produkte und -Technologie)*	• DCIM-USBG2



Hinweis: Die IBM BladeCenter-Modelle H und E müssen für die Unterstützung der automatischen Erkennung AMM mit der Firmwareversion BPET36K oder höher verwenden.

Hinweis: Bei den IBM-Blade-Center-Modellen E und H unterstützt der Dominion KX II nur die automatische Erkennung für AMM[1] als aktives primäres Verwaltungsmodul.

Erforderliche und empfohlene Blade-Chassis-Konfigurationen

Diese Tabelle enthält Informationen zu Beschränkungen, die für die Konfiguration von Blade-Chassis für Dominion KX II gelten. Raritan empfiehlt, die folgenden Informationen zu beachten.

Blade-Chassis	Erforderliche/empfohlene Aktion
Dell® PowerEdge® M1000e	• Deaktivieren Sie den iKVM-GUI-Bildschirmschoner. Ansonsten wird ein Autorisierungsdialogfenster angezeigt, wodurch das iKVM nicht korrekt funktioniert. • Verlassen Sie das iKVM-GUI-Menü, bevor Sie das Dell-Chassis an ein CIM von Raritan anschließen. Ansonsten funktioniert das iKVM möglicherweise nicht korrekt. • Konfigurieren Sie das Hauptmenü der iKVM-GUI so, dass Zielblades nach Slot und nicht nach Name ausgewählt werden. Ansonsten funktioniert das iKVM möglicherweise nicht korrekt. • Wählen Sie im Scan-Setupmenü der iKVM-GUI *keine* Slots für Scanvorgänge aus. Ansonsten funktioniert das iKVM möglicherweise nicht korrekt. • Wählen Sie im Scan-Broadcastmenü der iKVM-GUI *keine* Slots für Tastatur-/Maus-Broadcastvorgänge aus. Ansonsten funktioniert das iKVM möglicherweise nicht korrekt. • Legen Sie zum Aufrufen der iKVM-GUI eine einzelne Tastenfolge fest. Diese Tastenfolge muss auch während der Dominion KX II-Portkonfiguration identifiziert werden. Ansonsten kann dies zu ungewollten iKVM-Vorgängen aufgrund von Client-Zugriffstasteneingaben führen. • Stellen Sie sicher, dass "Front Panel USB/Video Enabled" (USB/Video auf Vorderseite aktiviert) bei der iKVM-Konfiguration über die Dell-CMC-GUI *nicht* ausgewählt wurde. Ansonsten haben Verbindungen über die Vorderseite des Chassis Priorität vor der Dominion KX II-Verbindung auf der Rückseite, sodass der iKVM-Betrieb nicht ordnungsgemäß funktioniert. Die Meldung "User has been disabled as front panel is currently active" (Der Benutzer wurde deaktiviert, da die Vorderseite zurzeit aktiv ist) wird angezeigt. • Stellen Sie sicher, dass "Allow access to CMC CLI from iKVM" (Zugriff auf CMC CLI vom iKVM zulassen) bei der iKVM-Konfiguration über die Dell-CMC-GUI *nicht* ausgewählt

Blade-Chassis	Erforderliche/empfohlene Aktion
	wurde. • Um zu verhindern, dass die iKVM-GUI bei der Verbindungsherstellung zum Blade-Chassis angezeigt wird, stellen Sie unter "Screen Delay Time" (Bildschirmverzögerungszeit) die Verzögerungszeit auf 8 Sekunden. • Es wird empfohlen, dass während des iKVM-GUI-Flagsetup die Optionen "Timed" (Abgestimmt) und "Displayed" (Angezeigt) ausgewählt werden. Dadurch können Sie die Verbindung zum gewünschten Bladeslot visuell bestätigen.
Dell PowerEdge 1855/1955	• Deaktivieren Sie den iKVM-GUI-Bildschirmschoner. Ansonsten wird ein Autorisierungsdialogfenster angezeigt, wodurch das iKVM nicht korrekt funktioniert. • Verlassen Sie das iKVM-GUI-Menü, bevor Sie das Dell-Chassis an ein CIM von Raritan anschließen. Ansonsten funktioniert das iKVM möglicherweise nicht korrekt. • Konfigurieren Sie das Hauptmenü der iKVM-GUI so, dass Zielblades nach Slot und nicht nach Name ausgewählt werden. Ansonsten funktioniert das iKVM möglicherweise nicht korrekt. • Wählen Sie im Scan-Setupmenü der iKVM-GUI *keine* Slots für Scanvorgänge aus. Ansonsten funktioniert das iKVM möglicherweise nicht korrekt. • Um zu verhindern, dass die iKVM-GUI bei der Verbindungsherstellung zum Blade-Chassis angezeigt wird, stellen Sie unter "Screen Delay Time" (Bildschirmverzögerungszeit) die Verzögerungszeit auf 8 Sekunden. • Es wird empfohlen, dass während des iKVM-GUI-Flagsetup die Optionen "Timed" (Abgestimmt) und "Displayed" (Angezeigt) ausgewählt werden. Dadurch können Sie die Verbindung zum gewünschten Bladeslot visuell bestätigen.
IBM®/Dell Auto-Discovery	• Es wird empfohlen, die automatische Erkennung zu aktivieren, wenn Sie Zugriffsberechtigungen auf Blade-Ebene anwenden. Ansonsten sollten Sie Zugriffsberechtigungen auf Blade-Chassis-Ebene vergeben. • Secure Shell (SSH) muss auf dem Verwaltungsmodul des Blade-Chassis aktiviert sein. • Der SSH-Port, der auf dem Managementmodul des Blade-Chassis konfiguriert, und die Portnummer, die auf der Seite "Port Configuration" (Portkonfiguration) eingegeben wurde, müssen übereinstimmen.
IBM KX2 Virtual Media	• Virtuelle Medien von Raritan Dominion KX II werden nur für die IBM BladeCenter®-Modelle H und E unterstützt. Dies erfordert die Verwendung des D2CIM-DVUSB. Der schwarze



Blade-Chassis	Erforderliche/empfohlene Aktion
	D2CIM-DVUS-USB-Niedriggeschwindigkeitsanschluss ist auf der Rückseite der Einheit mit dem Administrative Management Module (AMM) verbunden. Der graue D2CIM-DVUS-USB-Hochgeschwindigkeitsanschluss ist auf der Vorderseite der Einheit mit dem Media Tray (MT) verbunden. Dazu benötigen Sie ein USB-Verlängerungskabel.

Hinweis: Alle IBM BladeCenter, die AMM verwenden, müssen die AMM mit der Firmwareversion BPET36K oder höher verwenden, um Funktion mit Dominion KX II sicherzustellen.

Hinweis: Bei den IBM-Blade-Center-Modellen E und H unterstützt der Dominion KX II nur die automatische Erkennung für AMM[1] als aktives primäres Verwaltungsmodul.

Beispiel-URL-Formate für Blade-Chassis

Diese Tabelle enthält Beispiel-URL-Formate für Blade-Chassis, die in Dominion KX II konfiguriert wurden.

Blade-Chassis	Beispiel-URL-Format
Dell® M1000e	• URL: https://192.168.60.44/cgi-bin/webcgi/login • Benutzername: root • Benutzernamenfeld: user • Kennwort: calvin • Kennwortfeld: password
Dell 1855	• URL: https://192.168.60.33/Forms/f_login • Benutzername: root • Benutzernamenfeld: TEXT_USER_NAME • Kennwort: calvin • Kennwortfeld: TEXT_PASSWORD
IBM® BladeCenter® E oder H	• http://192.168.84.217/private/welcome.ssi



Konfigurieren von USB-Profilen (Seite "Port")

Im Abschnitt "Select USB Profiles for Port" (USB-Profile für Port auswählen) auf der Seite "Port" wählen Sie die verfügbaren USB-Profile für einen Port aus. Die auf der Seite "Port" ausgewählten USB-Profile sind die Profile, die für den Benutzer im VKC verfügbar sind, wenn von diesem Port eine Verbindung zu einem KVM-Zielserver hergestellt wird. Der Standard ist Windows 2000®, Windows XP®, Windows Vista®. Weitere Informationen zu USB-Profilen finden Sie unter ***USB-Profile*** (auf Seite 118).

Hinweis: Um USB-Profile für einen Port festzulegen, muss eine Verbindung zu einem VM-CIM bestehen, das über die Firmware verfügt, die mit der aktuellen Firmwareversion des Dominion KX II kompatibel ist. Siehe **Aktualisieren von CIMs** *(auf Seite 258)**.*

Die Profile, die für die Zuordnung zu einem Port verfügbar sind, werden in der Liste "Available" (Verfügbar) auf der linken Bildschirmseite angezeigt. Die Profile, die für die Verwendung mit einem Port ausgewählt wurden, werden in der Liste "Selected" (Ausgewählt) auf der rechten Bildschirmseite angezeigt. Wenn Sie in einer der Listen ein Profil auswählen, wird im Feld "Profile Description" (Profilbeschreibung) eine Beschreibung des Profils und dessen Verwendung angezeigt.

Neben der Auswahl einer Reihe von Profilen für einen KVM-Port können Sie außerdem das bevorzugte Profil für den Port angeben und die für einen Port festgelegten Einstellungen für andere KVM-Ports übernehmen.

Hinweis: Weitere Informationen zur Verwendung des Mac OS-X®-USB-Profils bei Verwendung von DCIM-VUSB oder DCIM-DVUSB finden Sie unter **Mausmodi bei Verwendung des Mac OS-X-USB-Profils mit einem DCIM-VUSB** *(siehe "***Mausmodi bei Verwendung des Mac OS-X-USB-Profils mit einem DCIM-VUSB.***" auf Seite 127)**.*

So öffnen Sie die Seite "Port":

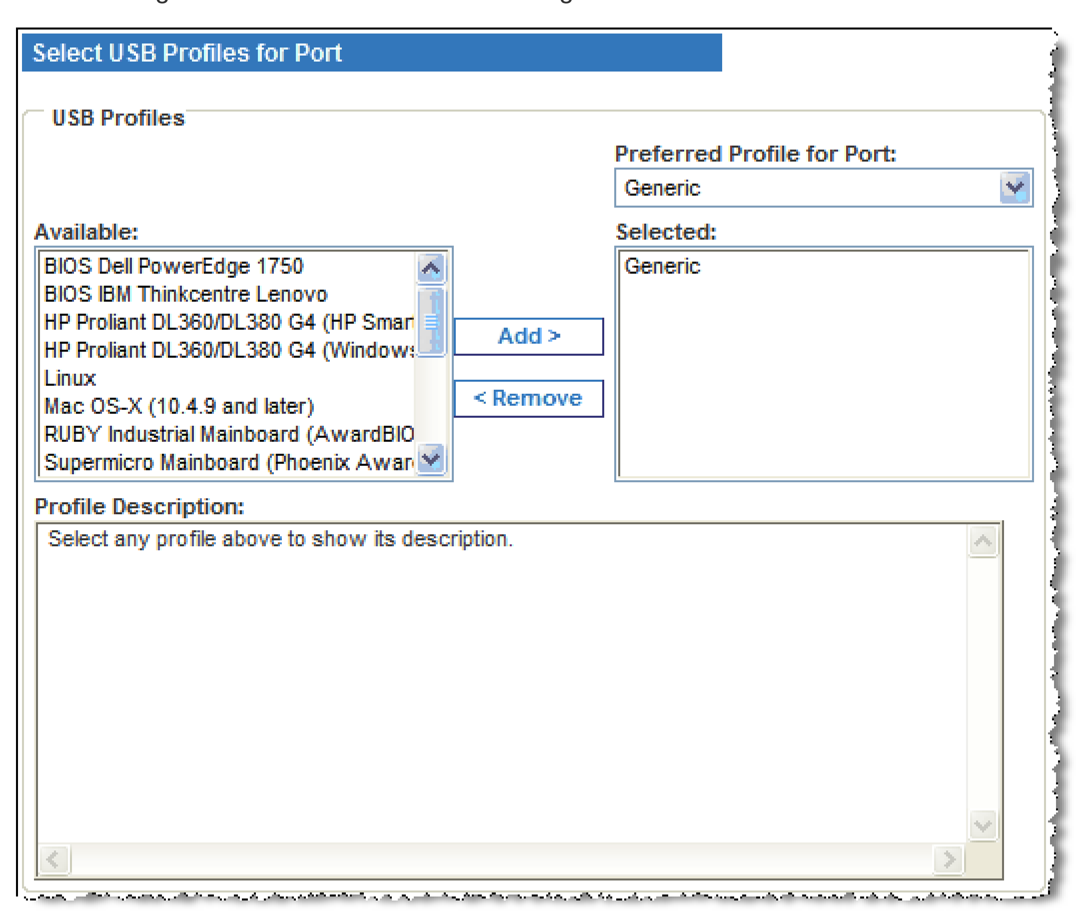
1. Wählen Sie "Device Settings" > "Port Configuration" (Geräteeinstellungen > Portkonfiguration) aus. Die Seite "Port Configuration" (Portkonfiguration) wird angezeigt.
2. Klicken Sie auf den Portnamen des KVM-Ports, den Sie bearbeiten möchten. Die Seite "Port" wird angezeigt.

So wählen Sie die USB-Profile für einen KVM-Port aus:

1. Wählen Sie im Abschnitt "Select USB Profiles for Port" (USB-Profile für Port auswählen) ein oder mehrere USB-Profile aus der Liste "Available" (Verfügbar) aus.



- Halten Sie die Umschalttaste gedrückt und wählen Sie mit der Maus die gewünschten aufeinander folgenden Profile aus.
- Halten Sie die Strg-Taste gedrückt und wählen Sie mit der Maus die gewünschten nicht aufeinander folgenden Profile aus.



2. Klicken Sie auf "Add" (Hinzufügen). Die ausgewählten Profile werden in der Liste "Selected" (Ausgewählt) angezeigt. Dies sind die Profile, die für den mit dem Port verbundenen KVM-Zielserver verwendet werden können.

So legen Sie ein bevorzugtes USB-Profil fest:

1. Nachdem Sie die verfügbaren Profile für einen Port ausgewählt haben, wählen Sie eines aus dem Menü "Preferred Profile for Port" (Bevorzugtes Profil für Port) aus. Standardmäßig ist das generische Profil festgelegt. Das ausgewählte Profil wird bei der Verbindungsherstellung zum KVM-Zielserver verwendet. Sie können bei Bedarf jedes andere USB-Profil verwenden.

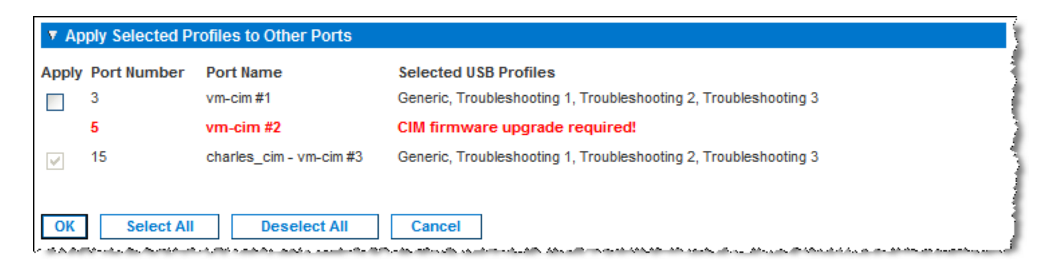


So entfernen Sie ausgewählte USB-Profile:

1. Wählen Sie im Abschnitt "Select USB Profiles for Port" (USB-Profile für Port auswählen) ein oder mehrere Profile aus der Liste "Selected" (Ausgewählt) aus.
   - Halten Sie die Umschalttaste gedrückt und wählen Sie mit der Maus die gewünschten aufeinander folgenden Profile aus.
   - Halten Sie die Strg-Taste gedrückt und wählen Sie mit der Maus die gewünschten nicht aufeinander folgenden Profile aus.
2. Klicken Sie auf "Remove" (Entfernen). Die ausgewählten Profile werden in der Liste "Available" (Verfügbar) angezeigt. Diese Profile sind nicht mehr für einen mit diesem Port verbundenen KVM-Zielserver verfügbar.

So übernehmen Sie eine Profilauswahl für mehrere Ports:

1. Aktivieren Sie im Abschnitt "Apply Selected Profiles to Other Ports" (Ausgewählte Profile für andere Ports übernehmen) das Kontrollkästchen "Apply" (Übernehmen) für alle KVM-Ports, für die Sie die aktuelle Auswahl an USB-Profilen übernehmen möchten.



   - Klicken Sie auf "Select All" (Alle auswählen), um alle KVM-Ports auszuwählen.
   - Klicken Sie auf "Deselect All" (Auswahl aufheben), um die Auswahl der KVM-Ports aufzuheben.



Lokale Porteinstellungen für Dominion KX II konfigurieren

Auf der Seite "Local Port Settings" (Lokale Porteinstellungen) können Sie viele Einstellungen für die lokale Dominion KX II-Konsole anpassen. Dazu zählen die Tastatur, die Zugriffstasten, die Verzögerung beim Videowechsel, der Stromsparmodus, die Auflösungseinstellungen für die lokale Benutzeroberfläche sowie die lokale Benutzerauthentifizierung. Außerdem können Sie ein USB-Profil vom lokalen Port ändern.

Für die Modelle KX2-832 und KX2-864 können Sie auf der Seite "Local Port Settings" (Lokale Porteinstellungen) den erweiterten lokalen Port konfigurieren. Der erweiterte lokale Port ist möglicherweise mit einem Paragon-Switch oder einer Paragon-User Station verbunden, um die Reichweite des lokalen Ports zu erweitern. Wie der Standardport lassen sich auch Tastatur, Zugriffstasten, Verzögerung beim Videowechsel, Stromsparmodus, Auflösungseinstellungen für die lokale Benutzeroberfläche und Einstellungen zur lokalen Benutzerauthentifizierung konfigurieren. Der erweiterte lokale Port kann von der lokalen und der Remote-Konsole aus konfiguriert werden. Weitere Informationen zum lokalen Standardport und zum erweiterten lokalen Port finden Sie unter ***Einstellungen zum lokalen Standardport und zum erweiterten lokalen Port bei den Geräten X2-832 und KX2-864*** (siehe "***Einstellungen zum lokalen Standardport und zum erweiterten lokalen Port für die Modelle KX2-832 und KX2-864***" auf Seite 230).

Hinweis: Ist der erweiterte lokale Port bei den Geräten KX2-832 und KX2-864 aktiviert und der Port frei, kommt es beim Umschalten auf ein Ziel über den lokalen Port zu einer Verzögerung von 2–3 Sekunden.

▶ So konfigurieren Sie die lokalen Porteinstellungen:

Hinweis: Einige Einstellungsänderungen, die auf der Seite "Local Port Settings" (Lokale Porteinstellungen) vorgenommen werden, führen zum Neustart des verwendeten Browsers. Führt eine Einstellungsänderung zum Neustart des Browser, so ist dies in den hier beschriebenen Schritten vermerkt.

1. Wählen Sie "Device Settings" > "Local Port Settings" (Geräteeinstellungen > Lokale Porteinstellungen) aus. Die Seite "Local Port Settings" (Lokale Porteinstellungen) wird angezeigt.
2. Aktivieren Sie das Kontrollkästchen neben "Enable Standard Local Port" (Lokalen Standardport aktivieren). Deaktivieren Sie das Kontrollkästchen, um den Port zu deaktivieren. Der lokale Standardport ist standardmäßig aktiviert, kann jedoch bei Bedarf aktiviert werden. Der Browser wird neu gestartet, nachdem diese Änderung durchgeführt wurde.Wenn Sie die Schichtfunktion verwenden, ist diese Funktion deaktiviert, da beide Funktionen nicht gleichzeitig verwendet werden können.



3. Wenn Sie ein KX2-832- oder KX2-864-Gerät verwenden, aktivieren Sie das Kontrollkästchen neben dem erweiterten lokalen Port, um diesen zu aktivieren. Deaktivieren Sie das Kontrollkästchen, um den Port zu deaktivieren. Wenn Sie die Smart Card-Funktion verwenden, muss der erweiterte lokale Port deaktiviert sein. Der Browser wird neu gestartet, nachdem diese Änderung durchgeführt wurde.

   Sind der lokale Standardport und der erweiterte lokale Port deaktiviert, kann auf die lokalen Ports nicht zugegriffen werden. Wenn Sie versuchen, über einen deaktivierten Port auf ein KX2-832- oder KX2-864-Gerät zuzugreifen, wird eine Meldung angezeigt, in der Sie darauf hingewiesen werden, dass das Gerät unter Remote-Verwaltung steht und die Anmeldefunktion deaktiviert ist.

   Hinweis: Wenn Sie KX2-832 und KX2-864 als Schichtgeräte verwenden, müssen Sie sie über den erweiterten lokalen Port an das Dominion KX II-Basisgerät anschließen.

   Hinweis: Wenn Sie ein Paragon-Gerät an den erweiterten Port eines der Modelle KX2-832 und KX2-864 anschließen, müssen Sie den Remoteclient verwenden, um das USB-Profil zu ändern.

4. Wenn Sie die Schichtfunktion verwenden, wählen Sie das Kontrollkästchen "Enable Local Port Device Tiering" (Geräteschicht für lokalen Port aktivieren) aus und geben den geheimen Schlüssel für die Schicht in das Feld "Tier Secret" (Geheimer Schlüssel der Schicht) ein. Um die Schichten zu konfigurieren, müssen Sie auch das Basisgerät auf der Seite "Device Services" (Gerätedienste) konfigurieren. Weitere Informationen zu Schichten finden Sie unter ***Konfigurieren und Aktivieren von Schichten*** (auf Seite 167).
5. Wählen Sie aus den Optionen in der Dropdown-Liste den geeigneten Tastaturtyp aus. Der Browser wird neu gestartet, nachdem diese Änderung durchgeführt wurde.
   - US (USA)
   - US/International (USA/International)
   - United Kingdom (Großbritannien)
   - French (France) (Französisch)
   - German (Germany) (Deutsch, Deutschland)
   - JIS (Japanese Industry Standard) [Japanisch (Japanischer Branchenstandard)]
   - Simplified Chinese (Vereinfachtes Chinesisch)
   - Traditional Chinese (Traditionelles Chinesisch)
   - Dubeolsik Hangul (Korean) (Koreanisch)
   - German (Deutsch, Schweiz)
   - Portugiesisch (Portugal)



- Norwegian (Norway) (Norwegisch)
- Swedish (Sweden) (Schwedisch)
- Danish (Denmark) (Dänisch)
- Belgian (Belgium) (Belgisch)

Hinweis: Sie können die Tastatur für Chinesisch, Japanisch und Koreanisch nur für die Anzeige verwenden. Für Funktionen der lokalen Dominion KX II-Konsole werden Eingaben in diesen Sprachen derzeit nicht unterstützt.

6. Wählen Sie die Zugriffstaste für den lokalen Port. Über die Zugriffstaste für den lokalen Port können Sie zur Benutzeroberfläche der lokalen Dominion KX II-Konsole zurückkehren, wenn gerade eine Zielserveroberfläche angezeigt wird. Die Standardoption lautet "Double Click Scroll Lock" (Rollen-Taste zweimal drücken). Sie können jedoch eine andere Tastenkombination aus der Dropdownliste auswählen.

Zugriffstaste	Zu drückende Tastenkombination
Rollen-Taste zweimal drücken	Drücken Sie die Rollen-Taste zweimal kurz hintereinander.
Num-Feststelltaste zweimal drücken	Drücken Sie die Num-Feststelltaste zweimal kurz hintereinander.
Feststelltaste zweimal drücken	Drücken Sie die Feststelltaste zweimal kurz hintereinander.
Linke Alt-Taste zweimal drücken	Drücken Sie die linke Alt-Taste zweimal kurz hintereinander.
Linke Umschalttaste zweimal drücken	Drücken Sie die linke Umschalttaste zweimal kurz hintereinander.
Linke Strg-Taste zweimal drücken	Drücken Sie die linke Strg-Taste zweimal kurz hintereinander.

7. Wählen Sie die Verbindungstaste für den lokalen Port aus. Verwenden Sie eine Verbindungstastenfolge, um eine Verbindung mit einem Zielgerät herzustellen und zu einem anderen Zielgerät zu wechseln. Sie können anschließend die Zugriffstaste verwenden, um die Verbindung zum Zielgerät zu trennen und zur GUI des lokalen Ports zurückzukehren. Die Verbindungstaste ist für Standardserver und Blade-Chassis verfügbar. Wenn die Verbindungstaste für den lokalen Port erstellt wurde, erscheint diese im Navigationsfenster der GUI, sodass Sie sie als Referenz verwenden können. Beispiele für Verbindungstastenfolgen finden Sie unter ***Beispiele für Verbindungstasten*** (auf Seite 294).

8. Legen Sie ggf. im Feld "Video Switching Delay" (Verzögerung beim Videowechsel) einen Wert zwischen 0 und 5 Sekunden fest. Üblicherweise wird der Wert 0 verwendet, wenn nicht mehr Zeit benötigt wird (manche Monitore benötigen mehr Zeit, um das Videobild zu wechseln).
9. Führen Sie die folgenden Schritte aus, wenn Sie die Stromsparfunktion verwenden möchten:
   a. Aktivieren Sie das Kontrollkästchen "Power Save Mode" (Stromsparmodus).
   b. Legen Sie die Zeitspanne (in Minuten) fest, nach der in den Stromsparmodus geschaltet wird.
10. Wählen Sie in der Dropdown-Liste die Auflösung für die lokale Dominion KX II-Konsole aus: Der Browser wird neu gestartet, nachdem diese Änderung durchgeführt wurde.
    - 800 x 600
    - 1024 x 768
    - 1280 x 1024
11. Wählen Sie in der Dropdown-Liste die Aktualisierungsfrequenz aus. Der Browser wird neu gestartet, nachdem diese Änderung durchgeführt wurde.
    - 60 Hz
    - 75 Hz
12. Wählen Sie die Methode zur lokalen Benutzerauthentifizierung aus:
    - Local/LDAP/RADIUS (Lokal/LDAP/RADIUS): Dies ist die empfohlene Option. Weitere Informationen zur Authentifizierung finden Sie unter ***Remoteauthentifizierung*** (auf Seite 40).
    - Keine. Der lokale Konsolenzugriff wird nicht authentifiziert. Diese Option ist nur für sichere Umgebungen empfehlenswert.
    - Aktivieren Sie das Kontrollkästchen "Ignore CC managed mode on local port" (Modus zur Verwaltung über CC auf lokalem Port ignorieren), wenn Sie den lokalen Benutzerzugriff auf Dominion KX II ermöglichen möchten, auch wenn das Gerät über CC-SG verwaltet wird.

Hinweis: Wenn diese Option deaktiviert ist, Sie sie später jedoch aktivieren möchten, müssen Sie die CC-SG-Verwaltung für das Gerät beenden (von CC-SG aus). Anschließend können Sie das Kontrollkästchen aktivieren.



Hinweis: Um den lokalen Standardport und den erweiterten lokalen Port zu verwenden, während Dominion KX II von CC-SG verwaltet wird, muss die Option "Ignore CC managed mode on local port" (Modus zur Verwaltung über CC auf lokalem Port ignorieren) ausgewählt werden. Aktivieren Sie das Kontrollkästchen "Ignore CC managed mode on local port" (Modus zur Verwaltung über CC auf lokalem Port ignorieren), wenn Sie lokalen Benutzerzugriff über den lokalen Standardport oder den erweiterten lokalen Port auf Dominion KX II ermöglichen möchten, wenn das Gerät über CC-SG verwaltet wird. Sie können auch den direkten Gerätezugriff verwenden, wenn die CC-SG-Verwaltungsfunktion aktiviert ist.

13. Klicken Sie auf OK.

Einstellungen zum lokalen Standardport und zum erweiterten lokalen Port für die Modelle KX2-832 und KX2-864

Die Modelle KX2-832 und KX2-864 bieten Ihnen zwei Optionen zu den lokalen Ports: Den lokalen Standardport und den erweiterten lokalen Port. Beide Port-Optionen werden über die Remotekonsole auf der Seite "Port Configuration" (Portkonfiguration) oder über die lokale Konsole auf der Seite "Local Port Settings" (Lokale Porteinstellungen) aktiviert bzw. deaktiviert. Weitere Informationen finden Sie unter ***Lokale Porteinstellungen für Dominion KX II konfigurieren*** (auf Seite 225).

Standardmäßig ist der lokale Standardport aktiviert und der erweiterte lokale Port deaktiviert. Wenn Sie die Reichweite des lokalen Ports erweitern möchten, aktivieren Sie den erweiterten lokalen Port, und verwenden Sie ein Kabel der Kategorie 5/5e/6, um ein DKX2-832- oder DKX2-864-Gerät mit einem Paragon II UMT, EUST, UST oder URKVMG zu verbinden.

Hinweis: Ist der erweiterte lokale Port bei den Geräten KX2-832 und KX2-864 aktiviert und der Port frei, kommt es beim Umschalten auf ein Ziel über den lokalen Port zu einer Verzögerung von 2–3 Sekunden

---

Um diese Optionen zu konfigurieren, müssen Sie über Administratorberechtigungen verfügen. Um einen Port zuzugreifen, müssen Sie nur einmal Ihren Benutzernamen und das Kennwort eingeben. Sie müssen diese Anmeldeinformationen nicht für jeden Port angeben, auf den Sie zugreifen.

Details zu den vom erweiterten lokalen Port unterstützten Geräten sowie zu den Entfernungsangaben und unterstützten CIMs finden Sie Abschnitt ***Spezifikationen*** (siehe "***Technische Daten***" auf Seite 304).

Verbindungsbeschränkungen bei den Modellen KX2-832und KX2-864

Lokaler Standardport und erweiterter lokaler Port greifen gleichzeitig auf ein Ziel zu. Lokaler Standardport und erweiterter lokaler Port nutzen Tastatur, Video und Maus gemeinsam, wenn beide aktiviert sind. Beide sind mit dem Ziel verbunden oder die Verbindung ist bei beiden unterbrochen.

Sobald entweder der lokale Standardport oder der erweiterte lokale Port deaktiviert ist, werden Tastatur, Video und Maus für die Ports deaktiviert. Es wird eine Meldung angezeigt, die darauf hinweist, dass die lokalen Ports deaktiviert wurden.



Kapitel 9 Sicherheitsverwaltung

In diesem Kapitel

Security Settings (Sicherheitseinstellungen)

Auf der Seite "Security Settings" (Sicherheitseinstellungen) können Sie Anmeldebeschränkungen angeben, Benutzer blockieren, Kennwortregeln festlegen und Daten verschlüsseln und freigeben.

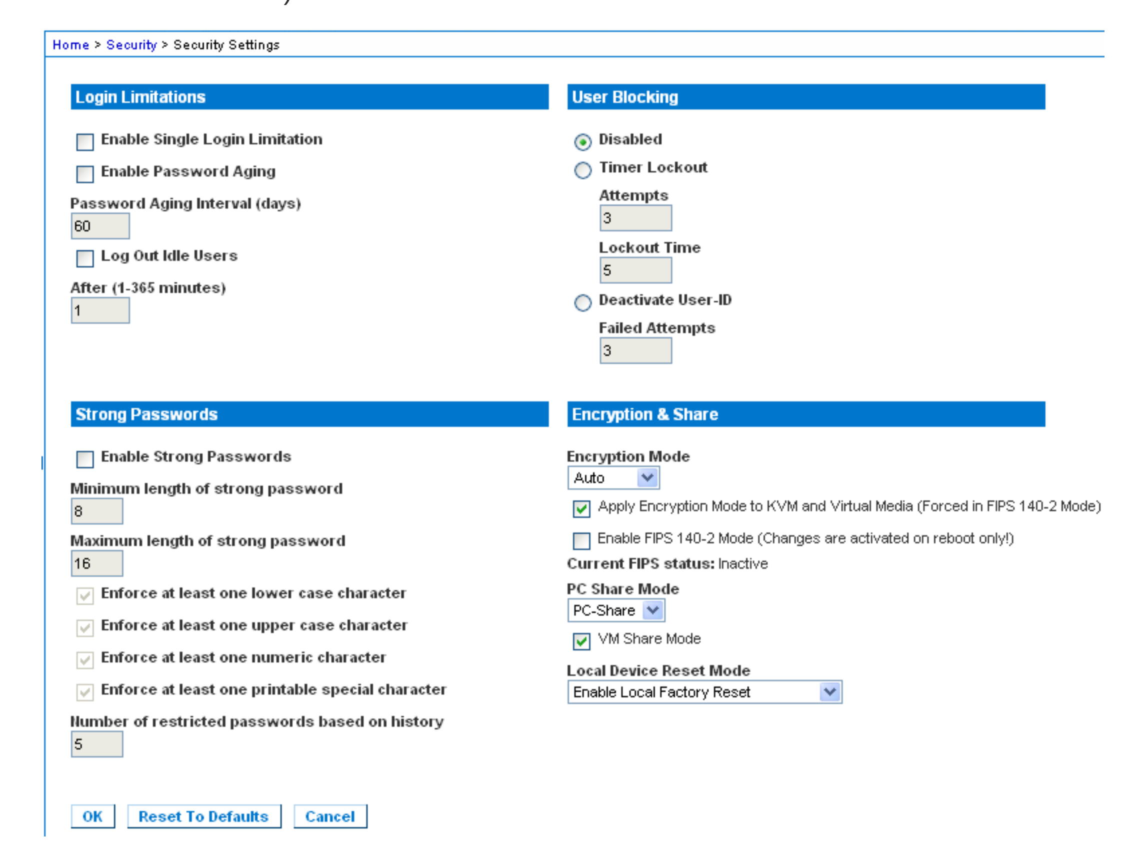
Für den Austausch öffentlicher und privater Schlüssel werden SSL-Zertifikate von Raritan verwendet, die zusätzliche Sicherheit bieten. Raritan-Webserverzertifikate sind selbstsigniert. Java-Applet-Zertifikate sind durch ein VeriSign-Zertifikat signiert. Die Verschlüsselung stellt sicher, dass Ihre Informationen nicht in falsche Hände geraten, und anhand dieser Zertifikate sehen Sie, dass es sich um Raritan, Inc. handelt.

► **So konfigurieren Sie die Sicherheitseinstellungen:**

1. Wählen Sie "Security" > "Security Settings" (Sicherheit > Sicherheitseinstellungen) aus. Die Seite "Security Settings" (Sicherheitseinstellungen) wird angezeigt.
2. Aktualisieren Sie ggf. die Einstellungen unter ***Login Limitations (Anmeldebeschränkungen)*** (siehe "***Anmeldebeschränkungen***" auf Seite 232).
3. Aktualisieren Sie ggf. die Einstellungen unter ***Strong Passwords (Sichere Kennwörter)*** (auf Seite 234).
4. Aktualisieren Sie ggf. die Einstellungen für ***User Blocking (Benutzersperrung)*** (auf Seite 235).
5. Aktualisieren Sie ggf. die Einstellungen unter Encryption & Share (Verschlüsselung und Freigabe).
6. Klicken Sie auf OK.

So stellen Sie die Standardwerte wieder her:

- Klicken Sie auf "Reset to Defaults" (Standardeinstellungen wiederherstellen).



Anmeldebeschränkungen

Mithilfe von Anmeldebeschränkungen können Sie Beschränkungen für Einzelanmeldungen, die Geltungsdauer von Kennwörtern und das Abmelden inaktiver Benutzer festlegen.

Beschränkung	Beschreibung
Enable single login limitation (Beschränkung für Einzelanmeldung aktivieren)	Wenn Sie dieses Kontrollkästchen aktivieren, ist pro Benutzername immer nur eine Anmeldung zulässig. Ist es dagegen deaktiviert, kann eine Benutzername-/Kennwortkombination von mehreren Client-Workstations gleichzeitig verwendet werden, um eine Verbindung mit dem Gerät herzustellen.
Enable password	Wenn Sie dieses Kontrollkästchen aktivieren,



Beschränkung	Beschreibung
aging (Kennworterneuerung aktivieren)	müssen alle Benutzer ihr Kennwort abhängig von der Anzahl der Tage, die Sie im Feld "Password Aging Interval" (Intervall für Kennworterneuerung) eingegeben haben, regelmäßig ändern. Dieses Feld ist aktiv und erforderlich, wenn Sie das Kontrollkästchen "Enable Password Aging" (Kennworterneuerung aktivieren) aktiviert haben. Geben Sie den Zeitraum in Tagen an, nach dessen Ablauf ein Kennwort geändert werden muss. Der Standardwert ist 60 Tage.
Log out idle users, After (1-365 minutes) (Inaktive Benutzer abmelden, Nach (1-365 Minuten))	Aktivieren Sie das Kontrollkästchen "Log off idle users" (Inaktive Benutzer abmelden), um die Verbindung von Benutzern automatisch zu trennen, wenn der im Feld "After (1-365 minutes)" [Nach (1-365 Minuten)] angegebene Zeitraum abgelaufen ist. Wenn keine Tastatur- oder Mausaktivitäten stattfinden, werden alle Sitzungen und Ressourcen abgemeldet. Für virtuelle Mediensitzungen gibt es hingegen kein Zeitlimit. Das Feld "After" (Nach) dient zum Festlegen der Zeitspanne (in Minuten), nach der ein inaktiver Benutzer abgemeldet wird. Dieses Feld ist aktiv, wenn das Kontrollkästchen "Log Out Idle Users" (Inaktive Benutzer abmelden) aktiviert wurde. Als Feldwert können bis zu 365 Minuten eingegeben werden.

Strong Passwords (Sichere Kennwörter)

Sichere Kennwörter sorgen für eine sicherere lokale Authentifizierung des Systems. Im Bereich "Strong Passwords" (Sichere Kennwörter) können Sie das Format gültiger lokaler Dominion KX II-Kennwörter wie Mindest- und Höchstlänge, erforderliche Zeichen und Aufbewahrung des Kennwortverlaufs festlegen.

Damit ein Kennwort sicher ist, muss es eine Mindestlänge von acht Zeichen haben sowie mindestens ein alphabetisches Zeichen und ein nicht-alphabetisches Zeichen (Satzzeichen oder Ziffer) umfassen. Darüber hinaus dürfen die ersten vier Zeichen des Kennworts und des Benutzernamens nicht identisch sein.

Wenn Sie diese Option aktivieren, gelten die Regeln für sichere Kennwörter. Benutzer, deren Kennwörter nicht den Kriterien für sichere Kennwörter entsprechen, werden bei der nächsten Anmeldung automatisch aufgefordert, ihr Kennwort zu ändern. Ist die Option deaktiviert, gilt nur die Standardformatvalidierung. Bei aktivierter Option sind die folgenden Felder aktiv und erforderlich:

Feld	Beschreibung
Minimum length of strong password (Mindestlänge des sicheren Kennworts)	Kennwörter müssen mindestens 8 Zeichen umfassen. Es dürfen aber bis zu 63 Zeichen sein.
Maximum length of strong password (Höchstlänge des sicheren Kennworts)	Die Standardlänge liegt bei 16 Zeichen, es dürfen aber bis zu 64 Zeichen sein.
Enforce at least one lower case character (Mindestens einen Kleinbuchstaben erzwingen)	Wenn diese Option aktiviert ist, muss das Kennwort mindestens einen Kleinbuchstaben enthalten.
Enforce at least one upper case character (Mindestens einen Großbuchstaben erzwingen)	Wenn diese Option aktiviert ist, muss das Kennwort mindestens einen Großbuchstaben enthalten.
Enforce at least one numeric character (Mindestens eine Ziffer erzwingen)	Wenn diese Option aktiviert ist, muss das Kennwort mindestens eine Ziffer enthalten.
Enforce at least one printable special character (Mindestens ein druckbares Sonderzeichen erzwingen)	Wenn diese Option aktiviert ist, muss das Kennwort mindestens ein (druckbares) Sonderzeichen enthalten.
Number of restricted passwords based on history (Anzahl unzulässiger	Dieses Feld bezieht sich auf die Verlaufstiefe, d. h. die Anzahl vorheriger Kennwörter, die nicht wiederholt werden



Feld	Beschreibung
Kennwörter basierend auf Verlauf)	dürfen. Ein Bereich zwischen 1 und 12 ist möglich, der Standardwert liegt bei 5.

User Blocking (Benutzersperrung)

Mithilfe der Optionen unter "User Blocking" (Benutzersperrung) geben Sie die Kriterien an, anhand derer Benutzer nach der festgelegten Zahl von Anmeldefehlversuchen am Zugriff auf das System gehindert werden.

Die drei Optionen schließen sich gegenseitig aus.

Option	Beschreibung
Disabled (Deaktiviert)	Dies ist die Standardoption. Benutzer werden unabhängig von der Anzahl fehlgeschlagener Anmeldeversuche nicht blockiert.

<table>
<tr><th>Option</th><th>Beschreibung</th></tr>
<tr><td>Timer Lockout (Zeitliche Sperre)</td><td>Benutzern wird der Zugriff auf das System für den festgelegten Zeitraum verweigert, nachdem sie eine bestimmte Anzahl fehlgeschlagener Anmeldeversuche überschritten haben. Bei dieser Option stehen die folgenden Felder zur Verfügung:
▪ Attempts (Versuche) – Geben Sie die Anzahl fehlgeschlagener Anmeldeversuche ein, nach der ein Benutzer gesperrt wird. Ein Bereich zwischen 1 und 10 ist möglich, der Standardwert liegt bei 3 Versuchen.
▪ Lockout Time (Dauer der Sperre) – Geben Sie die Zeitspanne ein, für die der Benutzer gesperrt wird. Ein Bereich zwischen 1 und 1440 Minuten ist möglich, der Standardwert liegt bei 5 Minuten.
Hinweis: Administratoren sind von einer zeitlichen Sperre ausgenommen.</td></tr>
<tr><td>Deactivate User-ID (Benutzer-ID deaktivieren)</td><td>Diese Option legt fest, dass dem Benutzer nach der Anzahl der im Feld "Failed Attempts" (Fehlversuche) angegebenen Anmeldefehlversuche der Zugriff auf das System verweigert wird:
▪ Failed Attempts (Fehlversuche) – Geben Sie die Anzahl der Anmeldefehlversuche ein, nach der die Benutzer-ID eines Benutzers deaktiviert wird. Dieses Feld steht zur Verfügung, wenn Sie die Option "Deactivate User-ID" (Benutzer-ID deaktivieren) wählen. Ein Bereich zwischen 1 und 10 ist möglich.</td></tr>
</table>

Wenn eine Benutzer-ID nach der angegebenen Anzahl der Anmeldefehlversuche deaktiviert wird, muss der Administrator das Benutzerkennwort ändern und das Benutzerkonto wieder aktivieren, indem er auf der Seite "User" (Benutzer) das Kontrollkästchen "Active" (Aktiv) aktiviert.



Encryption & Share (Verschlüsselung und Freigabe)

Mithilfe der Einstellungen unter "Encryption & Share" (Verschlüsselung und Freigabe) können Sie die Art der Verschlüsselung, PC- und VM-Freigabemodi sowie die Art der Zurücksetzung festlegen, wenn die Taste "Reset" (Zurücksetzen) an der Dominion KX II-Einheit gedrückt wird.

WARNUNG: Wenn Sie einen Verschlüsselungsmodus auswählen, der von Ihrem Browser nicht unterstützt wird, können Sie von Ihrem Browser aus nicht auf Dominion KX II zugreifen.

1. Wählen Sie eine Option aus der Dropdownliste "Encryption Mode" (Verschlüsselungsmodus) aus. Wenn Sie einen Verschlüsselungsmodus ausgewählt haben, wird eine Warnung angezeigt, dass Sie keine Verbindung zu Dominion KX II mehr herstellen können, falls Ihr Browser den gewählten Modus nicht unterstützt. Die Warnung lautet "When the Encryption Mode is specified please ensure that your browser supports this encryption mode; otherwise you will not be able to connect to the Dominion KX II" (Wenn Sie den Verschlüsselungsmodus festlegen, stellen Sie sicher, dass Ihr Browser diesen unterstützt, ansonsten können Sie keine Verbindung zu Dominion KX II herstellen).

Verschlüsselungsmodus	Beschreibung
Automatisch	Dies ist die empfohlene Option. Dominion KX II verwendet automatisch das höchstmögliche Verschlüsselungsniveau. Sie *müssen* "Auto" (Automatisch) auswählen, damit Gerät und Client erfolgreich die verwendeten FIPS-konformen Algorithmen verarbeiten können.
RC4	Sichert Benutzernamen, Kennwörter und KVM-Daten einschließlich Videoübertragungen mithilfe der Verschlüsselungsmethode "RSA RC4". Dies ist ein 128-Bit-SSL-Protokoll (Secure Sockets Layer), das während der Anfangsverbindungsauthentifizierung einen privaten Kommunikations-Channel zwischen dem Dominion KX II-Gerät und dem Remote-PC bereitstellt. Wenn Sie den Modus FIPS 140-2 aktivieren und RC4 ausgewählt wurde, erhalten Sie eine Fehlermeldung. Im Modus FIPS 140-2 ist RC4 nicht verfügbar.

Verschlüsselungsmodus	Beschreibung
AES-128	Der Advanced Encryption Standard (AES) ist eine Spezifikation des National Institute of Standards and Technology (USA) für die Verschlüsselung elektronischer Daten. 128 ist die Schlüssellänge. Achten Sie bei Auswahl dieser Option darauf, dass sie von Ihrem Browser unterstützt wird, da Sie sonst keine Verbindung herstellen können. Weitere Informationen finden Sie unter ***Prüfen Ihres Browsers auf AES-Verschlüsselung*** (auf Seite 240).
AES-256	Der Advanced Encryption Standard (AES) ist eine Spezifikation des National Institute of Standards and Technology (USA) für die Verschlüsselung elektronischer Daten. 256 ist die Schlüssellänge. Achten Sie bei Auswahl dieser Option darauf, dass sie von Ihrem Browser unterstützt wird, da Sie sonst keine Verbindung herstellen können. Weitere Informationen finden Sie unter ***Prüfen Ihres Browsers auf AES-Verschlüsselung*** (auf Seite 240).

Hinweis: Der MPC verwendet immer das höchste Verschlüsselungsniveau und entspricht der Einstellung unter "Encryption Mode" (Verschlüsselungsmodus), wenn diese nicht auf "Auto" eingestellt ist.

Hinweis: Wenn Sie Windows XP® mit Service Pack 2 verwenden, kann der Internet Explorer® 7 keine Remoteverbindung zu Dominion KX II herstellen, wenn die AES-128-Verschlüsselung verwendet wird.

2. Apply Encryption Mode to KVM and Virtual Media (Verschlüsselungsmodus auf KVM und virtuelle Medien anwenden): Wenn Sie dieses Kontrollkästchen aktivieren, wird der gewählte Verschlüsselungsmodus auf KVM und virtuelle Medien angewendet. Nach der Authentifizierung werden die KVM- und virtuellen Mediendaten ebenfalls mit der 128-Bit-Verschlüsselung übertragen.
3. Für das Arbeiten in Regierungs- und anderen Hochsicherheitsumgebungen muss der Modus FIPS 140-2 durch Aktivieren des Kontrollkästchens "Enable FIPS 140-2" (Aktivieren von FIPS 140-2) ausgewählt werden. Weitere Informationen zur Aktivierung von FIPS 140-2 finden Sie unter ***Aktivieren von FIPS 140-2*** (auf Seite 241).



4. PC Share Mode (PC-Freigabemodus): Bestimmt den globalen gleichzeitigen KVM-Remotezugriff und ermöglicht bis zu acht Remotebenutzern die gleichzeitige Anmeldung bei einer Dominion KX II-Einheit sowie die gleichzeitige Anzeige und Steuerung desselben Zielservers über das Gerät. Klicken Sie auf die Dropdownliste, um eine der folgenden Optionen auszuwählen:
   - Private (Privat) – Keine PC-Freigabe. Dies ist der Standardmodus. Jeder Zielserver ist jeweils nur für einen Benutzer exklusiv zugänglich.
   - PC-Share (PC-Freigabe) – Bis zu acht Benutzer (Administratoren oder Nicht-Administratoren) können gleichzeitig auf KVM-Zielserver zugreifen. Jeder Remotebenutzer besitzt dieselbe Kontrolle über Tastatur und Maus. Beachten Sie jedoch, dass eine ungleichmäßige Steuerung auftritt, wenn ein Benutzer seine Tastatur- bzw. Mauseingabe nicht unterbricht.
5. Wählen Sie bei Bedarf den Modus "VM Share" (VM-Freigabe) aus. Diese Option steht nur zur Verfügung, wenn der PC-Freigabemodus aktiviert wurde. Wenn dieses Kontrollkästchen aktiviert ist, werden virtuelle Medien für mehrere Benutzer freigegeben, d. h. diese können gemeinsam auf dieselbe virtuelle Mediensitzung zugreifen. Standardmäßig ist dieses Kontrollkästchen deaktiviert.
6. Aktivieren Sie bei Bedarf das Kontrollkästchen "Disable Local Port Output" (Lokalen Portausgang deaktivieren). Wenn dieses Kontrollkästchen aktiviert ist, werden auf dem lokalen Port keine Videodaten ausgegeben. Diese Einstellungen gelten nur für die Geräte KX2 832 und KX2 864. Wenn Sie Smart Card-Lesegeräte verwenden, *muss* der lokale Port deaktiviert sein.
7. Wählen Sie bei Bedarf den Modus "Local Device Reset" (Lokales Gerät zurücksetzen) aus. Diese Option legt fest, welche Maßnahmen ergriffen werden, wenn die Taste zum Zurücksetzen der Hardware auf der Rückseite des Geräts gedrückt wird. Weitere Informationen finden Sie unter Zurücksetzen von Dominion KX II mithilfe der Taste "Reset" (Zurücksetzen). Wählen Sie eine der folgenden Optionen aus:

Modus zum Zurücksetzen eines lokalen Geräts	**Beschreibung**
Enable Local Factory Reset (Lokale Werkrücksetzung aktivieren, Standardeinstellung)	Setzt das Dominion KX II-Gerät auf die werksseitigen Standardeinstellungen zurück.
Enable Local Admin Password Reset (Lokale Administrator-Kennwortrücksetzung	Setzt nur das Kennwort des lokalen Administrators zurück. Das Kennwort wird auf "raritan" zurückgesetzt.

Modus zum Zurücksetzen eines lokalen Geräts	Beschreibung
aktivieren)	
Disable All Local Resets (Alle lokalen Rücksetzungen deaktivieren)	Es wird keine Rücksetzungsmaßnahme ergriffen.

Hinweis: Wenn Sie P2CIM-AUSBDUAL oder P2CIM-APS2DUAL zum Anschließen eines Ziels an zwei Dominion KX II verwenden und der private Zugriff auf die Ziele erforderlich ist, muss für beide KVM-Switches die Option "Private" (Privat) als PC-Freigabemodus ausgewählt werden.

Zusätzliche Informationen zur Verwendung von Paragon CIMs mit Dominion KX II finden Sie unter ***Unterstützte Paragon-CIMS und Konfigurationen*** (auf Seite 315).

Prüfen Ihres Browsers auf AES-Verschlüsselung

Dominion KX II unterstützt AES-256. Falls Sie wissen möchten, ob Ihr Browser AES verwendet, erkundigen Sie sich beim Hersteller, oder navigieren Sie mithilfe des Browsers und der zu prüfenden Verschlüsselungsmethode zu folgender Website: https://www.fortify.net/sslcheck.html. Diese Website erkennt die Verschlüsselungsmethode Ihres Browsers und zeigt einen entsprechenden Bericht an.

Hinweis: Die AES-128-Bit- oder -256-Bit-Verschlüsselung wird vom Internet Explorer 6 nicht unterstützt.

Voraussetzungen und unterstützte Konfigurationen für die AES-256-Bit-Verschlüsselung

Die AES-256-Bit-Verschlüsselung wird nur von folgenden Webbrowsern unterstützt:

- Firefox® 2.0.0.x und 3
- Mozilla® 1.7.13
- Internet Explorer® 7 und 8

Für die AES-256-Bit-Verschlüsselung müssen außerdem die Sicherheitsrichtliniendateien für eine unbeschränkte Schlüssellänge der Java™ Cryptography Extension (JCE) installiert werden.

Diese sogenannten "Unlimited Strength Jurisdiction Policy Files" der verschiedenen JRE™-Versionen finden Sie unter folgendem Link im Bereich "Other Downloads" (Weitere Downloads):

- JRE1.6 - http://java.sun.com/javase/downloads/index_jdk5.jsp



Aktivieren von FIPS 140-2

Für das Arbeiten in Regierungs- und anderen Hochsicherheitsumgebungen ist es möglicherweise erforderlich, den Modus FIPS 140-2 zu aktivieren. Dominion KX II verfügt über ein integriertes FIPS 140-2-validiertes kryptografisches Modul, das gemäß Abschnitt G.5 der FIPS 140-2 Implementation Guidance auf einer Linux®-Plattform ausgeführt wird. Nach der Aktivierung dieses Moduls muss der private Schlüssel, der zur Generierung des SSL-Zertifikats verwendet wird, intern erzeugt werden. Dieser kann nicht heruntergeladen oder exportiert werden.

▶ So aktivieren Sie FIPS 140-2:

1. Öffnen Sie die Seite "Encryption & Share" (Verschlüsselung & Freigabe) (siehe ***Verschlüsselung & Freigabe*** (siehe "***Encryption & Share (Verschlüsselung und Freigabe)***" auf Seite 237)).
2. Aktivieren Sie den FIPS 140-2-Modus, indem Sie im Abschnitt "Encryption & Share" (Verschlüsselung & Freigabe) der Seite "Security Settings" (Sicherheitseinstellungen) das Kontrollkästchen "Enable FIPS 140-2" (Aktivieren von FIPS 140-2) aktivieren. Sie nutzen FIPS 140-2-zugelassene Algorithmen für die externe Kommunikation, sobald Sie sich im FIPS 140-2-Modus befinden. Das kryptografische FIPS-Modul wird für die Verschlüsselung von KVM-Sitzungsdaten verwendet. Dabei handelt es sich um Video-, Tastatur-, Maus- und Smart Card-Daten sowie um die Daten von virtuellen Medien.
3. Neustart der Dominion KX II-Einheit **Erforderlich**

   Sobald der FIPS-Modus aktiviert ist, wird im Abschnitt "Device Information" (Geräteinformationen) im linken Fenster der Bildschirmanzeige "FIPS Mode: Enabled" (FIPS-Modus aktiviert) angezeigt.

   Zusätzliche Sicherheit bietet das Erzeugen einer neuen Zertifikatsregistrierungsanforderung, nachdem der FIPS-Modus aktiviert wurde. Diese wird mithilfe des erforderlichen Schlüsselcodes erzeugt. Laden Sie das Zertifikat hoch, nachdem es signiert wurde, oder erzeugen Sie ein selbstsigniertes Zertifikat. Der SSL-Zertifikatstatus wird von "Not FIPS Mode Compliant" (Nicht FIPS-konform) zu "FIPS Mode Compliant" (FIPS-konform) aktualisiert.

   Ist der FIPS-Modus aktiviert, können keine Schlüsseldateien herunter- oder hochgeladen werden.   Die aktuell erzeugte CSR wird der Schlüsseldatei intern zugeordnet. Das SSL-Zertifikat der CA und der zugehörige private Schlüssel sind nicht in der vollständigen Wiederherstellung der gesicherten Datei enthalten. Der Schlüssel kann nicht von Dominion KX II exportiert werden.



Anforderungen für die Unterstützung von FIPS 140-2

Dominion KX II unterstützt FIPS 140-20-zugelassene Verschlüsselungsalgorithmen. Dadurch können SSL-Server und Client erfolgreich die für die verschlüsselte Sitzung verwendete Verschlüsselungsfolge verarbeiten, sobald ein Client exklusiv für den Modus FIPS 140-2 konfiguriert ist.

Im Folgenden finden Sie Hinweise zur Verwendung von FIPS 140-2 mit Dominion KX II:

Dominion KX II

- Nehmen Sie auf der Seite Security Settings (Sicherheitseinstellungen) für "Encryption & Share" (Verschlüsselung & Freigabe) die Einstellung auf "Auto" (Automatisch) vor. Siehe Encryption & Share (Verschlüsselung und Freigabe).

Microsoft-Client

- Am Client-Computer und im Internet Explorer muss "FIPS 140-2" aktiviert sein.

So aktivieren Sie "FIPS 140-2" auf einem Windows-Client:

1. Wählen Sie "Systemsteuerung" > "Verwaltung" > "Lokale Sicherheitsrichtline" aus, um das Dialogfeld "Lokale Sicherheitseinstellungen" zu öffnen.
2. Wählen Sie in der Navigationsstruktur "Lokale Richtlinien" > "Sicherheitsoptionen" aus.
3. Aktivieren Sie "Systemkryptografie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signierung verwenden".
4. Starten Sie den Client-Computer neu.

So aktivieren Sie "FIPS 140-2" im Internet Explorer:

1. Wählen Sie im Internet Explorer "Extras" > "Internetoptionen", und klicken Sie auf die Registerkarte "Erweitert".
2. Aktivieren Sie das Kontrollkästchen "TLS 1.0 verwenden".
3. Starten Sie den Browser neu.



Konfigurieren der IP-Zugriffssteuerung

Mithilfe der IP-Zugriffssteuerung können Sie den Zugriff auf Dominion KX II steuern. Durch das Einrichten einer globalen Zugriffssteuerungsliste (Access Control List, ACL) stellen Sie sicher, dass das Gerät nicht auf Pakete von unzulässigen IP-Adressen antwortet. Die IP-Zugriffssteuerung funktioniert global und betrifft die gesamte Dominion KX II-Einheit. Sie können den Zugriff auf das Gerät jedoch auch auf Gruppenebene steuern. Weitere Informationen zur Steuerung auf Gruppenebene finden Sie unter ***Gruppenbasierte IP-ACL (IP-Zugriffssteuerungsliste)*** (auf Seite 137).

Wichtig: Die IP-Adresse "127.0.0.1" wird vom lokalen Port der Dominion KX II-Einheit verwendet. Beim Erstellen der IP-Zugriffssteuerungsliste darf sich 127.0.0.1 nicht im Bereich der gesperrten IP-Adressen befinden, sonst können Sie nicht auf den lokalen Port der Dominion KX II-Einheit zugreifen.

So verwenden Sie die IP-Zugriffssteuerung:

1. Öffnen Sie die Seite "IP Access Control" (IP-Zugriffssteuerung), indem Sie "Security" > "IP Access Control" (Sicherheit > IP-Zugriffssteuerung) auswählen. Die Seite "IP Access Control" (IP-Zugriffssteuerung) wird angezeigt.
2. Aktivieren Sie das Kontrollkästchen "Enable IP Access Control" (IP-Zugriffssteuerung aktivieren), um die IP-Zugriffssteuerung sowie die restlichen Felder auf der Seite zu aktivieren.
3. Wählen Sie unter "Default Policy" (Standardrichtlinie) eine der im Folgenden genannten Optionen. Damit legen Sie fest, welche Maßnahme für IP-Adressen, die außerhalb der von Ihnen festgelegten Bereiche liegen, ergriffen werden soll.
   - Accept (Akzeptieren) – Diese IP-Adressen können auf das Dominion KX II-Gerät zugreifen.
   - Drop (Ablehnen) – Diesen IP-Adressen wird der Zugriff auf das Dominion KX II-Gerät verweigert.

   Hinweis: Sowohl IPv4- als auch IPv6-Adressen werden unterstützt.

So fügen Sie Regeln hinzu:

1. Geben Sie die IP-Adresse und die Subnetzmaske im Feld "IPv4/Mask" (IPv4/Maske) oder "Pv6/Prefix Length" (Pv6/Präfixlänge) ein.

   Hinweis: Die IP-Adresse sollte unter Verwendung der CIDR-Notation (Classless Inter-Domain Routing) eingegeben werden. (Hierbei werden die ersten 24 Bits als Netzwerkadresse verwendet.)



2. Wählen Sie in der Dropdownliste "Policy" (Richtlinie) eine Richtlinie aus.
3. Klicken Sie auf "Append" (Anfügen). Die Regel wird unten in der Liste hinzugefügt.

▶ So fügen Sie eine Regel ein:

1. Geben Sie im Feld "Rule #" (Regelnummer) eine Regelnummer ein. Diese ist für den Befehl "Insert" (Einfügen) erforderlich.
2. Geben Sie die IP-Adresse und die Subnetzmaske im Feld "IPv4/Mask" (IPv4/Maske) oder "Pv6/Prefix Length" (Pv6/Präfixlänge) ein.
3. Wählen Sie in der Dropdownliste "Policy" (Richtlinie) eine Richtlinie aus.
4. Klicken Sie auf "Insert" (Einfügen). Wenn die eingegebene Regelnummer einer bereits vorhandenen entspricht, wird die neue Regel vor der vorhandenen Regel eingefügt, und alle Regeln werden um eine Position nach unten verschoben.

Tipp: Mithilfe der Regelnummern können Sie die Reihenfolge, in der die Regeln erstellt werden, besser steuern.

▶ So ersetzen Sie eine Regel:

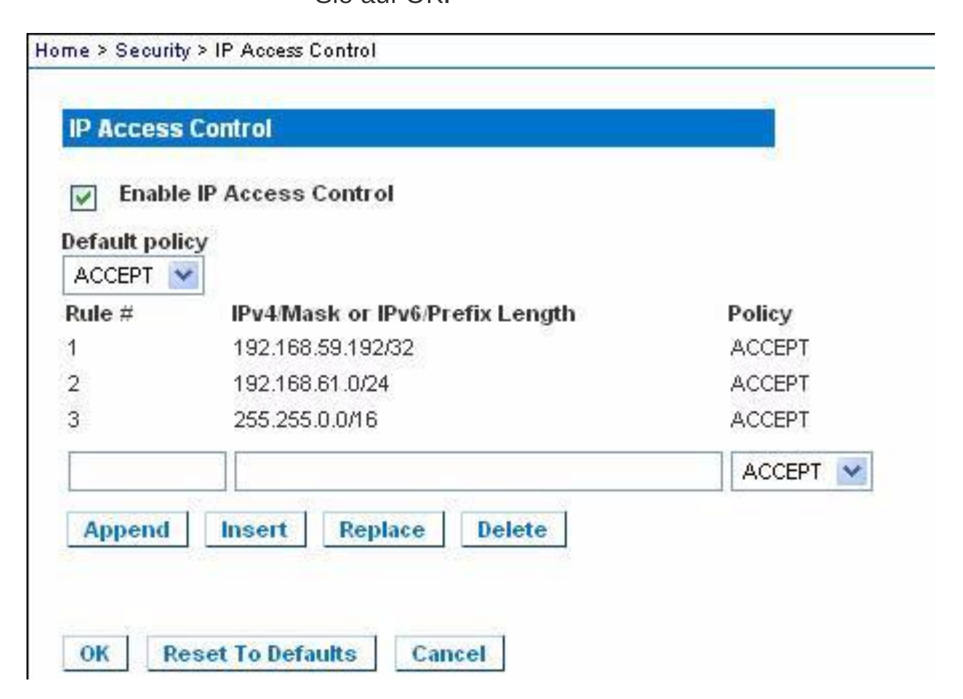
1. Geben Sie die zu ersetzende Regelnummer an.
2. Geben Sie die IP-Adresse und die Subnetzmaske im Feld "IPv4/Mask" (IPv4/Maske) oder "Pv6/Prefix Length" (Pv6/Präfixlänge) ein.
3. Wählen Sie in der Dropdownliste "Policy" (Richtlinie) eine Richtlinie aus.
4. Klicken Sie auf "Replace" (Ersetzen). Ihre neue Regel ersetzt die ursprüngliche Regel mit derselben Regelnummer.

▶ So löschen Sie eine Regel:

1. Geben Sie die zu löschende Regelnummer an.
2. Klicken Sie auf "Delete" (Löschen).



3. Sie werden aufgefordert, den Löschvorgang zu bestätigen. Klicken Sie auf OK.



SSL-Zertifikate

Das SSL-Protokoll (Secure Socket Layer) wird für den gesamten verschlüsselten Netzwerkdatenverkehr zwischen Dominion KX II und einem mit der Einheit verbundenen Client verwendet. Wenn eine Verbindung hergestellt wird, muss sich Dominion KX II gegenüber einem Client, der ein kryptografisches Zertifikat verwendet, identifizieren.

Es kann eine Zertifikatsregistrierungsanforderung (Certificate Signing Request, CSR) erzeugt und ein von der Zertifizierungsstelle (Certificate Authority, CA) signiertes Zertifikat auf dem Dominion KX II-Gerät installiert werden. Die CA prüft die Identität des Absenders der CSR. Anschließend sendet die CA ein signiertes Zertifikat an den Absender. Das Zertifikat mit der Signatur der renommierten CA wird verwendet, um für die Identität des Zertifikatsinhabers zu bürgen.

Certificate Signing Request (CSR)

Common name

Organizational unit

Organization

Locality/City

State/Province

Country (ISO code)

Email

Challenge password

Confirm Challenge password

Key length (bits)

1024 *

Create

* Stored value is equal to the default.



So erstellen und installieren Sie ein SSL-Zertifikat:

1. Wählen Sie "Security" > "SSL Certificate" (Sicherheit > SSL-Zertifikat) aus.
2. Füllen Sie die folgenden Felder aus:
   a. Common Name (Allgemeiner Name) – Der Netzwerkname der Dominion KX II-Einheit, wenn diese im Benutzernetzwerk installiert wurde (normalerweise der vollqualifizierte Domainname). Dieser ist mit dem Namen identisch, der für den Zugriff auf Dominion KX II über einen Webbrowser verwendet wird, allerdings ohne das Präfix "http://". Sollte der hier angegebene Name nicht dem tatsächlichen Netzwerknamen entsprechen, wird im Browser eine Sicherheitswarnung angezeigt, wenn über HTTPS auf Dominion KX II zugegriffen wird.
   b. Organizational Unit (Organisationseinheit) – In diesem Feld wird angegeben, zu welcher Abteilung der Organisation das Dominion KX II-Gerät gehört.
   c. Organization (Organisation) – Der Name der Organisation, zu der das Dominion KX II-Gerät gehört.
   d. Locality/City (Lokalität/Stadt) – Die Stadt, in der sich die Organisation befindet.
   e. State/Province (Bundesland/Region) – Das Bundesland oder die Region, in dem/der sich die Organisation befindet.
   f. Country (ISO code) [Land (ISO-Code)] – Das Land, in dem sich die Organisation befindet. Der ISO-Code ist der aus zwei Buchstaben bestehende Code der Internationalen Organisation für Normung, z. B. "DE" für Deutschland oder "US" für die USA.
   g. Challenge Password (Challenge-Kennwort) – Einige Zertifizierungsstellen verlangen ein Challenge-Kennwort für die Authentifizierung von späteren Änderungen des Zertifikats (z. B. Widerruf des Zertifikats). Die Mindestlänge dieses Kennworts beträgt vier Zeichen.
   h. Confirm Challenge Password (Challenge-Kennwort bestätigen) – Bestätigung des Challenge-Kennworts.
   i. Email (E-Mail) – Die E-Mail-Adresse einer Kontaktperson, die für Dominion KX II und dessen Sicherheit verantwortlich ist.
   j. Key Length (Schlüssellänge) – Die Länge des erzeugten Schlüssels in Bits. Die Standardlänge ist 1024.
3. Klicken Sie auf "Create" (Erstellen), um die Zertifikatsregistrierungsanforderung (Certificate Signing Request, CSR) zu erzeugen.



So laden Sie ein CSR-Zertifikat herunter:

1. Sie können die CSR und die Datei, die den bei der Erzeugung verwendeten privaten Schlüssel enthalten, herunterladen, indem Sie auf die Schaltfläche "Download" (Herunterladen) klicken.

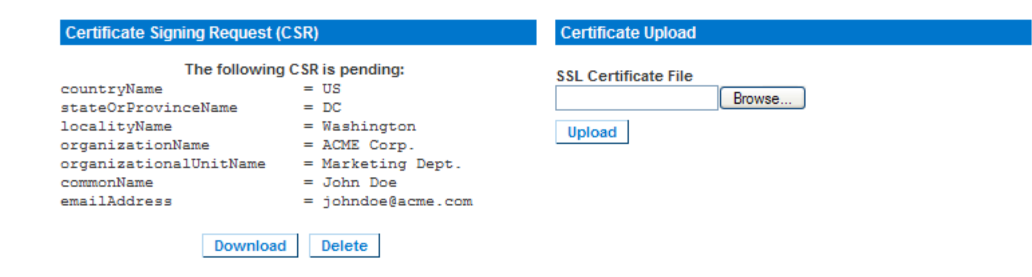
   Hinweis: Die CSR und die Datei für den privaten Schlüssel gehören zusammen und sollten auch dementsprechend verwendet werden. Wenn das signierte Zertifikat nicht mit dem bei der Erzeugung der ursprünglichen CSR verwendeten privaten Schlüssel übereinstimmt, kann das Zertifikat nicht verwendet werden. Dies gilt für das Hoch- und Herunterladen der CSR und den Dateien für den privaten Schlüssel.

2. Senden Sie die gespeicherte CSR zur Zertifizierung an eine Zertifizierungsstelle. Sie erhalten von dieser das neue Zertifikat.

So laden Sie eine CSR hoch:

1. Laden Sie das Zertifikat für Dominion KX II hoch, indem Sie auf die Schaltfläche "Upload" (Hochladen) klicken.

   Hinweis: Die CSR und die Datei für den privaten Schlüssel gehören zusammen und sollten auch dementsprechend verwendet werden. Wenn das signierte Zertifikat nicht mit dem bei der Erzeugung der ursprünglichen CSR verwendeten privaten Schlüssel übereinstimmt, kann das Zertifikat nicht verwendet werden. Dies gilt für das Hoch- und Herunterladen der CSR und den Dateien für den privaten Schlüssel.



Nach Abschluss dieser drei Schritte verfügt Dominion KX II über ein eigenes Zertifikat zur Identifizierung gegenüber den Clients.

Wichtig: Wenn Sie die CSR auf der Dominion KX II-Einheit löschen, kann diese nicht wiederhergestellt werden. Wenn Sie sie versehentlich gelöscht haben, müssen Sie die drei oben beschriebenen Schritte erneut durchführen. Um dies zu vermeiden, verwenden Sie die Downloadfunktion, sodass Sie über eine Kopie der CSR und des privaten Schlüssels verfügen.



Sicherheitsmeldung

Dominion KX II ermöglicht Ihnen, eine Sicherheitsmeldung zum Anmeldeprozess von Dominion KX II hinzuzufügen. Wenn diese Funktion aktiviert ist, müssen Benutzer vor dem Zugriff auf >ProductName< die Sicherheitsvereinbarung akzeptieren oder ablehnen. Die in einer Sicherheitsmeldung enthaltenen Informationen werden im Dialogfeld "Restricted Service Agreement" (Eingeschränkte Dienstvereinbarung) angezeigt, nachdem Benutzer nach Eingabe Ihrer Anmeldeinformationen auf Dominion KX II zugegriffen haben.

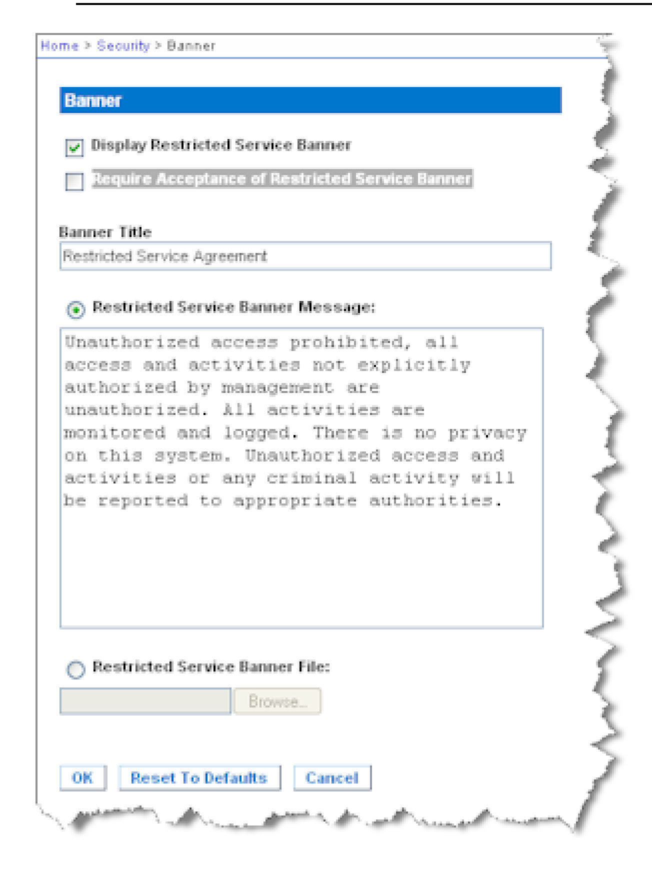
Die Überschrift und der Text der Sicherheitsmeldung kann angepasst werden, oder Sie können den Standardtext verwenden. Die Sicherheitsmeldung kann auch so konfiguriert werden, dass Benutzer die Sicherheitsvereinbarung akzeptieren müssen, bevor sie auf Dominion KX II zugreifen, oder die Sicherheitsmeldung kann einfach nach dem Anmeldevorgang angezeigt werden. Wenn die Funktion zum Akzeptieren oder Ablehnen aktiviert ist, wird die Auswahl des Benutzers im Prüfprotokoll protokolliert.

So konfigurieren Sie eine Sicherheitsmeldung:

1. Klicken Sie auf "Security" > "Banner" (Sicherheit > Meldung), um die Seite "Banner" (Meldung) zu öffnen.
2. Wählen Sie "Display Restricted Service Banner" (Meldung für eingeschränkten Dienst anzeigen) aus, um die Funktion zu aktivieren.
3. Wenn Benutzer die Meldung vor dem Anmeldeprozess bestätigen sollen, wählen Sie "Require Acceptance of Restricted Service Banner" (Akzeptieren der Meldung für eingeschränkten Dienst erforderlich) aus. Um die Meldung zu akzeptieren, müssen Benutzer ein Kontrollkästchen aktivieren. Wenn Sie diese Einstellung nicht aktivieren, wird die Sicherheitsmeldung nach der Anmeldung des Benutzers nur angezeigt. In diesem Fall ist keine Bestätigung durch den Benutzer erforderlich.
4. Ändern Sie ggf. den Namen der Meldung. Diese Informationen werden den Benutzern als Teil der Meldung angezeigt. Es können bis zu 64 Zeichen verwendet werden.
5. Bearbeiten Sie die Informationen im Textfeld "Restricted Services Banner" (Meldung zum eingeschränkten Dienst). Sie können maximal 6000 Zeichen eingeben oder eine Textdatei hochladen. Führen Sie hierfür einen der folgenden Schritte aus:
   a. Bearbeiten Sie den Text, indem Sie manuell in das Textfeld tippen. Klicken Sie auf OK.

b. Laden Sie Informationen aus einer .txt-Datei hoch, indem Sie das Optionsfeld "Restricted Services Banner File" (Datei für Sicherheitsmeldung für eingeschränkte Dienste) auswählen und auf "Browse" (Durchsuchen) klicken, um die Datei zu suchen und hochzuladen. Klicken Sie auf OK. Nachdem die Datei hochgeladen wurde, wird der Text aus der Datei im Textfeld "Restricted Services Banner Message" (Meldung zum eingeschränkten Dienst) angezeigt.

Hinweis: Eine Textdatei kann nicht vom lokalen Port hochgeladen werden.





Kapitel 10 Wartung

In diesem Kapitel

Prüfprotokoll

Alle Dominion KX II-Systemereignisse werden protokolliert.

So zeigen Sie das Prüfprotokoll für Ihre Dominion KX II-Einheit an:

1. Wählen Sie **Maintenance > Audit Log** (Wartung > Prüfprotokoll). Die Seite "Audit Log" (Prüfprotokoll) wird angezeigt.

   Die Seite "Audit Log" (Prüfprotokoll) enthält Ereignisse sortiert nach Datum und Uhrzeit, wobei die letzten Ereignisse zuerst aufgeführt werden. Das Prüfprotokoll enthält die folgenden Informationen:

   - Date (Datum) – Datum und Uhrzeit des Ereignisses, basierend auf dem 24-h-Zeitformat.
   - Event (Ereignis) – Der Ereignisname, wie er auf der Seite "Event Management" (Ereignisverwaltung) aufgeführt wird.
   - Description (Beschreibung) – Detaillierte Beschreibung des Ereignisses.

So speichern Sie das Prüfprotokoll:

Hinweis: Sie können das Prüfprotokoll nur mithilfe der Dominion KX II-Remotekonsole speichern, nicht jedoch mit der lokalen Konsole.

1. Klicken Sie auf "Save to File" (Speichern unter). Ein Dialogfeld zum Speichern der Datei wird angezeigt.
2. Wählen Sie einen Dateinamen und Speicherort aus, und klicken Sie auf "Save" (Speichern). Das Prüfprotokoll wird mit dem festgelegten Namen lokal am ausgewählten Ort auf dem Client-Computer gespeichert.



So blättern Sie durch das Prüfprotokoll:

- Verwenden Sie die Links **[Older]** ([Älter]) und **[Newer]** ([Neuer]).

Device Information (Geräteinformationen)

Die Seite "Device Information" (Geräteinformationen) enthält detaillierte Angaben zu Ihrem Dominion KX II-Gerät und den verwendeten CIMs. Diese Informationen benötigen Sie, wenn Sie sich mit dem technischen Kundendienst von Raritan in Verbindung setzen.

So zeigen Sie Informationen zu Ihrer Dominion KX II-Einheit und den CIMs an:

- Wählen Sie "Maintenance" > "Device Information" (Wartung > Geräteinformationen) aus. Die Seite "Device Information" (Geräteinformationen) wird angezeigt.

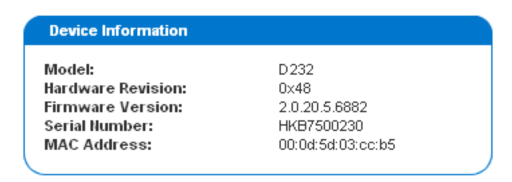
Zu der Dominion KX II-Einheit werden folgende Informationen angezeigt:

- Model (Modell)
- Hardware Revision (Hardware-Revision)
- Firmware Version (Firmware-Version)
- Serial Number (Seriennummer)
- MAC Address (MAC-Adresse)

Zu den verwendeten CIMs werden folgende Informationen angezeigt:

- Port (Number) [Port (Nummer)]
- Name
- Type of CIM (CIM-Typ) – DCIM, PCIM, Powerstrip oder VM
- Firmware Version (Firmware-Version)
- Serial Number (Seriennummer)

Home > Maintenance > Device Information Logout



CIM Information

▲ Port	Name	Type	Firmware Version	Serial Number
1	Dominion	VM	2A5D	HUW7250867
8	PwrStrip	PowerStrip	00B4	PQ16A00058



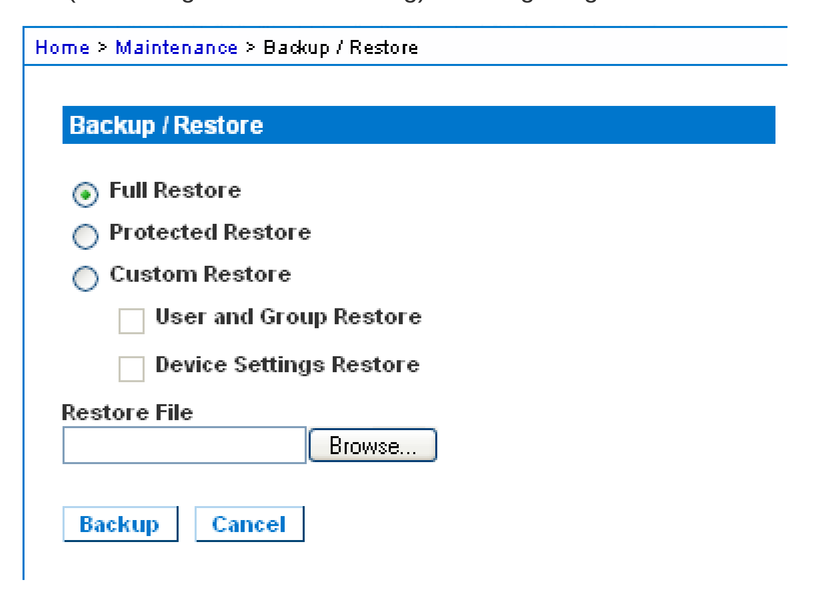
Backup and Restore (Sicherung und Wiederherstellung)

Auf der Seite "Backup/Restore" (Sicherung/Wiederherstellung) können Sie die Einstellungen und die Konfiguration der Dominion KX II-Einheit sichern und wiederherstellen.

Dieses Feature dient nicht nur der Gewährleistung der Geschäftskontinuität, Sie können damit auch viel Zeit sparen. So können Sie Ihrem Team beispielsweise schnell von einer anderen Dominion KX II-Einheit aus Zugriff gewähren, indem Sie die Benutzerkonfigurationseinstellungen des verwendeten Dominion KX II-Geräts sichern und auf dem neuen Dominion KX II-Gerät wiederherstellen. Sie können auch eine Dominion KX II-Einheit einrichten und deren Konfiguration auf mehrere andere Dominion KX II-Geräte kopieren.

So greifen Sie auf die Seite "Backup/Restore" (Sicherung/Wiederherstellung) zu:

- Wählen Sie "Maintenance" > "Backup/Restore" (Wartung > Sicherung/Wiederherstellung) aus. Die Seite "Backup/Restore" (Sicherung/Wiederherstellung) wird angezeigt.



Hinweis: Es wird immer das komplette System gesichert. Bei der Wiederherstellung können Sie zwischen einer vollständigen und einer teilweise durchgeführten Wiederherstellung wählen.

Wenn Sie Firefox® oder Internet Explorer® 5 (oder älter) zur Sicherung Ihres Dominion KX II verwenden:

1. Klicken Sie auf "Backup" (Sichern). Das Dialogfeld "File Download" (Dateidownload) wird angezeigt.



2. Klicken Sie auf "Save" (Speichern). Das Dialogfeld "Save As" (Speichern unter) wird angezeigt.
3. Wählen Sie einen Speicherort aus, geben Sie einen Dateinamen an und klicken Sie auf "Save" (Speichern). Das Dialogfeld "Download Complete" (Download abgeschlossen) wird angezeigt.
4. Klicken Sie auf "Close" (Schließen). Die Sicherungsdatei wird unter dem festgelegten Namen lokal am ausgewählten Ort auf dem Client-Computer gespeichert.

Wenn Sie Internet Explorer 6 (oder höher) zur Sicherung Ihres Dominion KX II verwenden:

1. Klicken Sie auf "Backup" (Sichern). Das Dialogfeld "File Download" (Dateidownload) mit der Schaltfläche "Open" (Öffnen) wird angezeigt. Klicken Sie nicht auf "Open" (Öffnen).

   Bei Internet Explorer 6 (oder höher) wird Internet Explorer als Standardanwendung zum Öffnen von Dateien verwendet. Sie werden aufgefordert, die Datei zu öffnen oder sie zu speichern. Um dies zu verhindern, müssen Sie eine Änderung vornehmen, sodass Wordpad als Standardanwendung zum Öffnen von Dateien verwendet wird.

2. Dies funktioniert wie folgt:
   a. Speichern Sie die Sicherungsdatei. Die Sicherungsdatei wird unter dem festgelegten Namen lokal am ausgewählten Ort auf dem Client-Computer gespeichert.
   b. Ist die Datei gespeichert, navigieren Sie zu dieser und klicken mit der rechten Maustaste darauf. Klicken Sie im dem Kontextmenü auf "Eigenschaften".
   c. Klicken Sie auf der Registerkarte "Allgemein" auf die Schaltfläche "Ändern", und wählen Sie im angezeigten Dialogfeld "Wordpad" aus.



So stellen Sie die Dominion KX II-Einheit wieder her:

> WARNUNG: Gehen Sie bei der Wiederherstellung Ihrer Dominion KX II-Einheit auf eine frühere Version vorsichtig vor. Die bei der Sicherung gespeicherten Benutzernamen und Kennwörter werden wiederhergestellt. Wenn Sie sich nicht mehr an die alten Anmeldedaten für den Administrator erinnern können, wird Ihnen der Zugriff auf die Dominion KX II-Einheit verweigert.
>
> Falls Sie zum Zeitpunkt der Sicherung eine andere IP-Adresse verwendet haben, wird auch diese wiederhergestellt. Wenn Sie DHCP konfiguriert haben, sollten Sie diesen Vorgang nur ausführen, wenn Sie Zugriff auf den lokalen Port haben, um nach der Aktualisierung die IP-Adresse zu prüfen.

1. Wählen Sie eine Wiederherstellungsart aus:

- Full Restore (Vollständige Wiederherstellung) – Das gesamte System wird wiederhergestellt. Wird normalerweise für herkömmliche Sicherungs- und Wiederherstellungszwecke verwendet.
- Protected Restore (Geschützte Wiederherstellung) – Alle Daten werden wiederhergestellt, mit Ausnahme von gerätespezifischen Informationen wie IP-Adresse, Name usw. Mit dieser Option können Sie eine Dominion KX II-Einheit einrichten und deren Konfiguration auf mehrere andere Dominion KX II-Geräte kopieren.
- Custom Restore (Benutzerdefinierte Wiederherstellung) – Bei dieser Option stehen Ihnen die Kontrollkästchen "User and Group Restore" (Wiederherstellung von Benutzern und Gruppen) und "Device Settings Restore" (Wiederherstellung der Geräteeinstellungen) zur Auswahl zur Verfügung.
  - User and Group Restore (Wiederherstellung von Benutzern und Gruppen) – Diese Option umfasst nur Benutzer- und Gruppeninformationen. Bei dieser Option werden das Zertifikat und die Dateien für den privaten Schlüssel *nicht* wiederhergestellt. Verwenden Sie diese Option, um schnell Benutzer auf einem anderen Dominion KX II-Gerät einzurichten.
  - Device Settings Restore (Wiederherstellung der Geräteeinstellungen) – Diese Option umfasst nur Geräteeinstellungen wie Stromzuordnungen, USB-Profile, Konfigurationsparameter hinsichtlich Blade-Chassis sowie Portgruppenzuordnungen. Verwenden Sie diese Option, um schnell die Geräteinformationen zu kopieren.

1. Klicken Sie auf "Browse" (Durchsuchen). Das Dialogfeld "Choose File" (Datei auswählen) wird angezeigt.

2. Navigieren Sie zur gewünschten Sicherungsdatei, markieren Sie sie, und klicken Sie auf "Open" (Öffnen). Die ausgewählte Datei wird im Feld "Restore File" (Datei wiederherstellen) aufgeführt.
3. Klicken Sie auf "Restore" (Wiederherstellen). Die Konfiguration wird basierend auf der gewählten Wiederherstellungsart wiederhergestellt.

USB Profile Management (USB-Profilverwaltung)

Auf der Seite "USB Profile Management" (USB-Profilverwaltung) können Sie benutzerdefinierte Profile hochladen, die vom technischen Kundendienst von Raritan bereitgestellt werden. Diese Profile dienen zur Erfüllung der Anforderungen Ihrer Zielserverkonfiguration, falls die verfügbaren Standardprofile diese nicht erfüllen. Der technische Kundendienst von Raritan stellt die benutzerdefinierten Profile bereit und hilft Ihnen bei der Erstellung einer Lösung für die speziellen Anforderungen Ihres Zielservers.

So öffnen Sie die Seite "USB Profile Management" (USB-Profilverwaltung):

- Wählen Sie > "Maintenance" > "USB Profile Management" (Wartung > USB-Profilverwaltung) aus. Die Seite "USB Profile Management" (USB-Profilverwaltung) wird geöffnet.



So laden Sie ein benutzerdefiniertes Profil auf Ihr Dominion KX II-Gerät:

1. Klicken Sie auf die Schaltfläche "Browse" (Durchsuchen). Das Dialogfeld "Choose File" (Datei auswählen) wird angezeigt.
2. Navigieren Sie zur gewünschten Datei des benutzerdefinierten Profils, markieren Sie sie und klicken Sie auf "Open" (Öffnen). Die ausgewählte Datei wird im Feld "USB Profile File" (USB-Profildatei) aufgeführt.



3. Klicken Sie auf "Upload" (Hochladen). Das benutzerdefinierte Profil wird hochgeladen und in der Tabelle "Profile" (Profil) angezeigt.

Hinweis: Wenn während des Ladevorgangs eine Fehlermeldung oder Warnung angezeigt wird [z. B. "Overwriting an existing custom profile" (Ein bestehendes benutzerdefiniertes Profil wird überschrieben)], können Sie den Ladevorgang fortsetzen, indem Sie auf "Upload" (Hochladen) klicken, oder abbrechen, indem Sie auf "Cancel" (Abbrechen) klicken.

So löschen Sie ein benutzerdefiniertes Profil von Ihrem Dominion KX II-Gerät:

1. Aktivieren Sie das Kontrollkästchen, das zu der Zeile der Tabelle gehört, in der das zu löschende benutzerdefinierte Profil aufgeführt ist.
2. Klicken Sie auf "Delete" (Löschen). Das benutzerdefinierte Profil wird gelöscht und aus der Tabelle "Profile" (Profil) entfernt.

Wie bereits erwähnt, können Sie ein benutzerdefiniertes Profil vom System löschen, auch wenn es noch als aktives Profil festgelegt ist. Dadurch werden alle bestehenden virtuellen Mediensitzungen beendet.

Handhaben von Konflikten bei Profilnamen

Ein Namenskonflikt zwischen benutzerdefinierten und Standard-USB-Profilen kann beim Durchführen einer Firmwareaktualisierung entstehen. Dies kann auftreten, wenn ein benutzerdefiniertes Profil, das erstellt und in die Liste der Standardprofile aufgenommen wurde, über den gleichen Namen verfügt wie ein neues USB-Profil, das im Rahmen der Firmwareaktualisierung heruntergeladen wird.

In diesem Fall wird das bereits bestehende benutzerdefinierte Profil mit dem Zusatz "old_" versehen. Wenn beispielsweise ein benutzerdefiniertes Profil mit dem Namen "GenericUSBProfile5" erstellt wurde und ein Profil mit dem gleichen Namen während einer Firmwareaktualisierung heruntergeladen wird, wird die bestehende Datei in "old_GenericUSBProfile5" umbenannt.

Sie können das bestehende Profil ggf. löschen. Weitere Informationen finden Sie unter ***USB Profile Management (USB-Profilverwaltung)*** (auf Seite 256).

Aktualisieren von CIMs

Gehen Sie wie unten beschrieben vor, um CIMs mithilfe der im Speicher des Dominion KX II-Geräts abgelegten Firmwareversionen zu aktualisieren. Im Allgemeinen werden alle CIMs aktualisiert, wenn Sie die Gerätefirmware über die Seite Firmware Upgrade (Firmwareaktualisierung) aktualisieren.

Um USB-Profile nutzen zu können, müssen Sie ein D2CIM-VUSB oder ein D2CIM-DVUSB mit aktualisierter Firmware verwenden. Ein VM-CIM ohne aktualisierte Firmware unterstützt eine große Anzahl an Konfigurationen (Windows®, Tastatur, Maus, CD-ROM und Wechselmedium), kann jedoch nicht die für bestimmte Zielkonfigurationen optimierten Profile nutzen. Daher sollten bestehende VM-CIMs mit der neuesten Firmware aktualisiert werden, um auf USB-Profile zugreifen zu können. Solange bestehende VM-CIMs noch nicht aktualisiert wurden, verfügen sie über eine Funktionalität, die dem generischen Profil entspricht.

Hinweis: Nur D2CIM-VUSB kann auf dieser Seite aktualisiert werden.

▶ So aktualisieren Sie CIMs mithilfe des Dominion KX II-Speichers:

1. Wählen Sie "Maintenance" > "CIM Firmware Upgrade" (Wartung > CIM-Firmwareaktualisierung) aus. Die Seite "CIM Firmware Upgrade" (CIM-Firmwareaktualisierung) wird geöffnet.

   Sie erkennen die CIMs leicht an den Angaben in den Feldern "Port", "Name", "Type" (Typ), "Current CIM Version" (Aktuelle CIM-Version) und "Upgrade CIM Version" (Neue CIM-Version).

2. Aktivieren Sie für alle CIMs, die aktualisiert werden sollen, das Kontrollkästchen "Selected" (Ausgewählt).

   Tipp: Verwenden Sie die Schaltflächen "Select All" (Alle auswählen) und "Deselect All" (Auswahl aufheben), um schnell alle CIMs auszuwählen bzw. diese Auswahl aufzuheben.

3. Klicken Sie auf die Schaltfläche "Upgrade" (Aktualisieren). Sie werden aufgefordert, die Aktualisierung zu bestätigen.
4. Klicken Sie auf OK, um fortzufahren. Während des Vorgangs werden Statusleisten angezeigt. Die Aktualisierung dauert maximal zwei Minuten pro CIM.



Aktualisieren der Firmware

Auf der Seite "Firmware Upgrade" (Firmwareaktualisierung) können Sie die Firmware von Dominion KX II und allen damit verbundenen CIMs aktualisieren. Diese Seite ist nur in der Dominion KX II-Remotekonsole verfügbar.

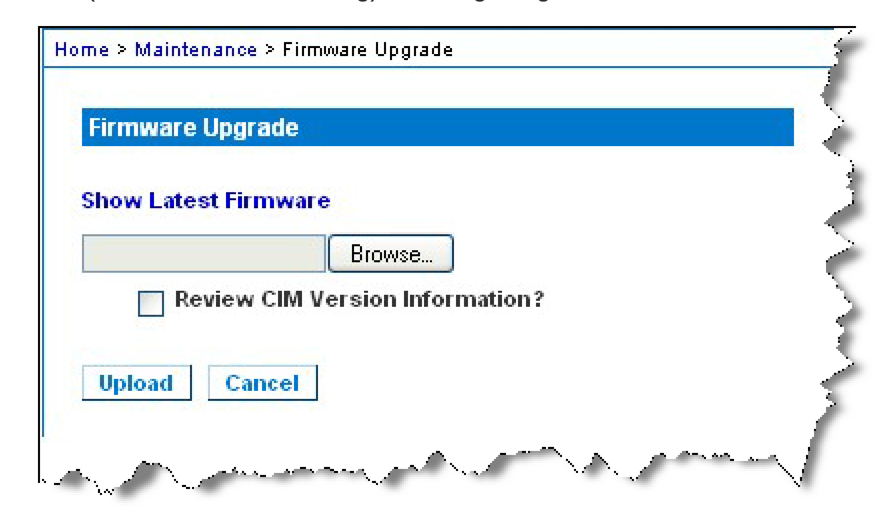
Wichtig: Schalten Sie während der Aktualisierung die Dominion KX II-Einheit nicht aus und trennen Sie nicht die Verbindung zu den CIMs, da dies zu Schäden an der Einheit bzw. den CIMs führen könnte.

- **So aktualisieren Sie die Dominion KX II-Einheit:**

1. Suchen Sie die entsprechende Raritan-Firmwaredistributionsdatei (*.RFP) auf der Seite für Firmwareaktualisierungen der ***Raritan-Website http://www.raritan.com***.
2. Entpacken Sie die Datei. Lesen Sie alle Anweisungen in den Firmware-ZIP-Dateien sorgfältig durch, bevor Sie die Aktualisierung durchführen.

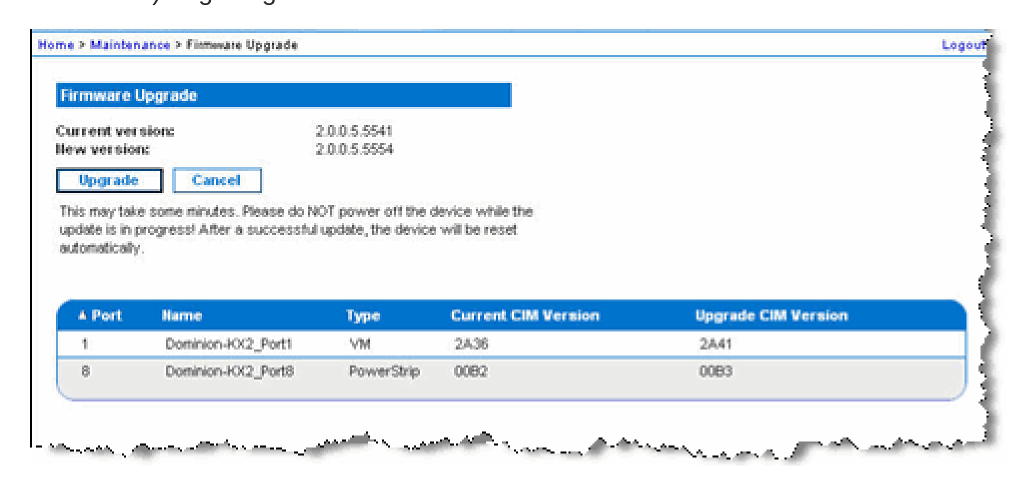
   Hinweis: Kopieren Sie die Firmwareaktualisierungsdatei vor dem Hochladen auf einen lokalen PC. Laden Sie die Datei nicht von einem Netzwerklaufwerk.

3. Wählen Sie "Maintenance" > "Firmware Upgrade" (Wartung > Firmwareaktualisierung) aus. Die Seite "Firmware Upgrade" (Firmwareaktualisierung) wird angezeigt.



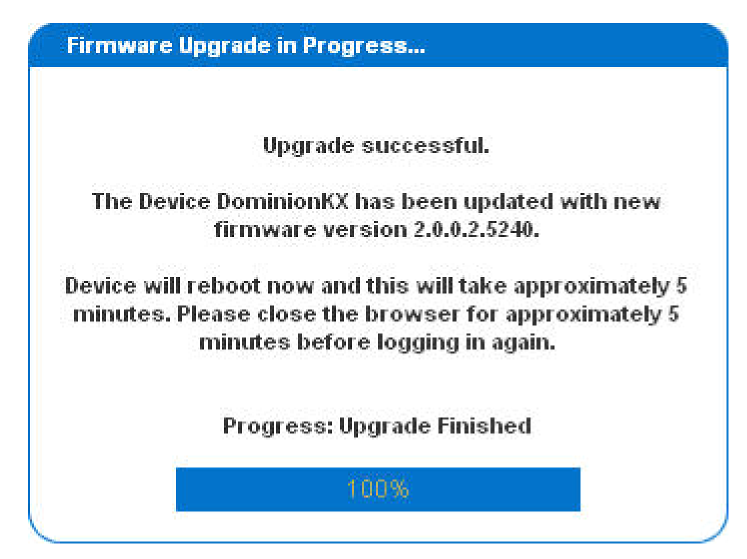
4. Klicken Sie auf die Schaltfläche "Browse" (Durchsuchen), um zu dem Verzeichnis zu navigieren, in dem Sie die Aktualisierungsdatei entpackt haben.

5. Aktivieren Sie das Kontrollkästchen "Review CIM Version Information?" (CIM-Versionsinformationen überprüfen?), wenn Informationen zu den Versionen der verwendeten CIMs angezeigt werden sollen.
6. Klicken Sie auf der Seite "Firmware Upgrade" (Firmwareaktualisierung) auf "Upload" (Hochladen). Ihnen werden Informationen zur Aktualisierung und den Versionsnummern sowie zu den CIMs (falls Sie das entsprechende Kontrollkästchen aktiviert haben) angezeigt.



Hinweis: Zu diesem Zeitpunkt werden verbundene Benutzer abgemeldet, und neue Anmeldeversuche werden blockiert.

7. Klicken Sie auf "Upgrade" (Aktualisieren). Warten Sie, bis der Vorgang abgeschlossen ist. Während des Vorgangs werden Statusinformationen und Statusleisten angezeigt. Nach Abschluss der Aktualisierung wird die Einheit neu gestartet (ein Tonsignal zeigt an, dass der Neustart abgeschlossen ist).





8. Schließen Sie den Browser, wenn Sie dazu aufgefordert werden, und warten Sie ungefähr fünf Minuten, bevor Sie sich erneut bei der Dominion KX II-Einheit anmelden.

Informationen zum Aktualisieren der Gerätefirmware mithilfe des Multi-Platform-Clients finden Sie im Benutzerhandbuch **KVM and Serial Access Clients Guide**.

Hinweis: Firmwareaktualisierungen über Modem werden nicht unterstützt.

Hinweis: Wenn Sie eine Schichtkonfiguration verwenden, in der ein Dominion KX II-Basisgerät für den Zugriff auf mehrere andere Schichtgeräte verwendet wird, wird möglicherweise eine Warnung wegen unzureichender Speicherkapazität während einer Firmwareaktualisierung angezeigt, wenn Sie viele Benutzergruppen verwenden. Wenn dieser Fehler angezeigt wird, starten Sie das Gerät neu, und führen Sie die Aktualisierung erneut aus. Wenn dieser Fehler nach dem Neustart weiterhin angezeigt wird, deaktivieren Sie die Schichten auf dem Basisgerät, und führen Sie die Aktualisierung erneut aus.



Upgrade History (Aktualisierungsverlauf)

Dominion KX II liefert Informationen über die Aktualisierungen, die auf Dominion KX II und den angeschlossenen CIMs durchgeführt wurden.

▶ So zeigen Sie den Aktualisierungsverlauf an:

- Wählen Sie "Maintenance" > "Upgrade History" (Wartung > Aktualisierungsverlauf) aus. Die Seite "Upgrade History" (Aktualisierungsverlauf) wird angezeigt.

Es werden Informationen zu den ausgeführten Dominion KX II-Aktualisierungen, dem Endstatus der Aktualisierung, den Start- und Abschlusszeiten sowie den vorherigen und aktuellen Firmwareversionen angezeigt. Es werden außerdem Informationen zu den CIMs bereitgestellt. Diese können angezeigt werden, indem Sie auf den Link der entsprechenden Aktualisierung klicken. Die folgenden CIM-Informationen stehen zur Verfügung:

- Type (Typ) – Der CIM-Typ
- Port – Der Port, an dem das CIM angeschlossen ist.
- User (Benutzer) – Der Benutzer, der die Aktualisierung durchgeführt hat.
- IP – IP-Adresse der Firmware
- Start Time (Startzeit) – Startzeit der Aktualisierung
- End Time (Abschlusszeit) – Abschlusszeit der Aktualisierung
- Previous Version (Vorherige Version – Vorherige CIM-Firmwareversion
- Upgrade Version (Neue Version) – Aktuelle CIM-Firmwareversion
- CIMs – Aktualisierte CIMs
- Result (Ergebnis) – Das Ergebnis der Aktualisierung (erfolgreich oder fehlgeschlagen)



Type	User	IP	Start Time	End Time	Previous Version	Upgrade Version	CIM's	Result
Full Firmware Upgrade	admin	192.168.59.63	June 16, 2008 14:15	June 16, 2008 14:23	2.0.20.5.6882	2.0.20.5.6926	show	Successful
Full Firmware Upgrade	admin	192.168.59.80	May 22, 2008 17:49	May 22, 2008 17:56	2.0.20.1.6853	2.0.20.5.6882	show	Successful



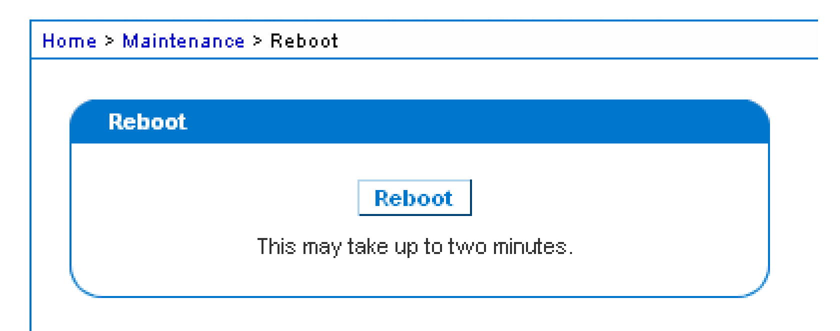
Neustart

Auf der Seite "Reboot" (Neustart) können Sie Dominion KX II auf sichere und kontrollierte Weise neustarten. Dies ist die empfohlene Methode zum Neustarten.

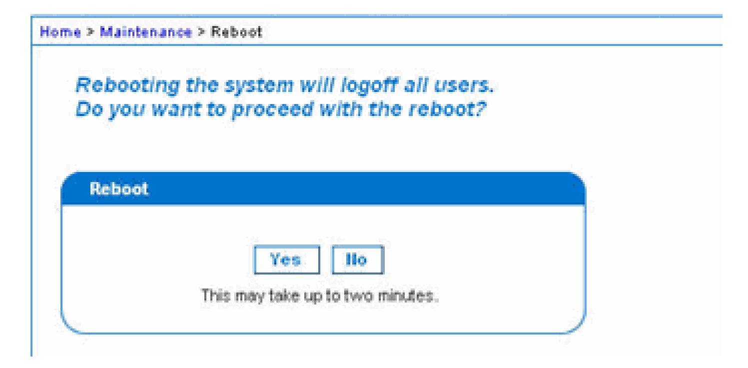
Wichtig: Alle seriellen und KVM-Verbindungen werden getrennt und alle Benutzer abgemeldet.

So starten Sie Dominion KX II neu:

1. Wählen Sie "Maintenance" > "Reboot" (Wartung > Neustart) aus. Die Seite "Reboot" (Neustart) wird angezeigt.



2. Klicken Sie auf "Reboot" (Neustart). Sie werden aufgefordert, die Aktion zu bestätigen. Klicken Sie auf "Yes" (Ja), um fortzufahren.



Beenden der CC-SG-Verwaltung

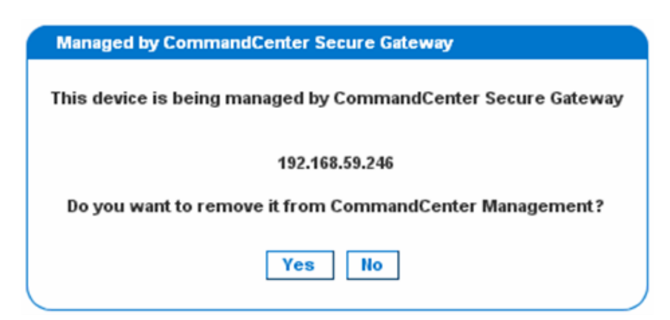
Wenn Dominion KX II von CC-SG verwaltet wird und Sie direkt auf das Gerät zugreifen möchten, erhalten Sie eine Meldung, dass das Gerät von CC-SG verwaltet wird.

Wenn Dominion KX II über CC-SG verwaltet und die Verbindung zwischen CC-SG und Dominion KX II nach Ablauf des festgelegten Zeitlimits (normalerweise 10 Minuten) getrennt wird, können Sie die CC-SG-Verwaltungssitzung über die Dominion KX II-Konsole beenden.

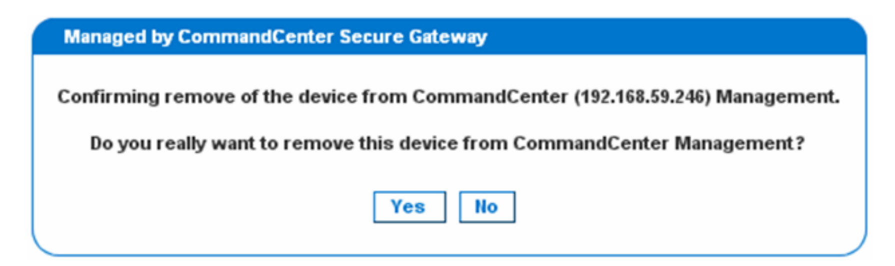
Hinweis: Sie müssen über die entsprechenden Berechtigungen zum Beenden der CC-SG-Verwaltung des Dominion KX II verfügen. Die Option "Stop CC-SG Management" (CC-SG-Verwaltung beenden) steht nur zur Verfügung, wenn Sie zurzeit CC-SG für die Verwaltung von Dominion KX II verwenden.

▶ So beenden Sie die CC-SG-Verwaltung eines Dominion KX II-Geräts:

1. Klicken Sie auf "Maintenance" > "Stop CC-SG Management" (Wartung > CC-SG-Verwaltung beenden). Eine Meldung, dass das Gerät von CC-SG verwaltet wird, wird angezeigt. Ebenso wird eine Option zum Beenden der CC-SG-Verwaltung für das Gerät angezeigt.



2. Klicken Sie auf "Yes" (Ja), um den Vorgang zum Beenden der CC-SG-Verwaltung für das Gerät zu starten. Eine Bestätigungsmeldung wird angezeigt, in der Sie aufgefordert werden, das Beenden der CC-SG-Verwaltung für das Gerät zu bestätigen.





3. Klicken Sie auf "Yes" (Ja), um die CC-SG-Verwaltung für das Gerät zu beenden. Wenn die CC-SG-Verwaltung beendet wurde, wird eine Bestätigungsmeldung angezeigt.

Managed by CommandCenter Secure Gateway

Stop CC-SG Management is successful. The device is no longer under CC-SG Management mode.

Ok



Kapitel 11 Diagnostics (Diagnose)

In diesem Kapitel

Seite "Network Interface" (Netzwerkschnittstelle)

Dominion KX II liefert Informationen zum Status der Netzwerkschnittstelle.

► **So zeigen Sie Informationen zur Netzwerkschnittstelle an:**

- Wählen Sie "Diagnostics > Network Interface" (Diagnose > Netzwerkschnittstelle) aus. Die Seite "Network Interface" (Netzwerkschnittstelle) wird angezeigt.

Diese Seite enthält die folgenden Informationen:

- Funktionsfähigkeit der Ethernet-Schnittstelle
- Erreichbarkeit des Gateways
- Derzeit aktiver LAN-Port

► **So aktualisieren Sie diese Informationen:**

- Klicken Sie auf die Schaltfläche "Refresh" (Aktualisieren).

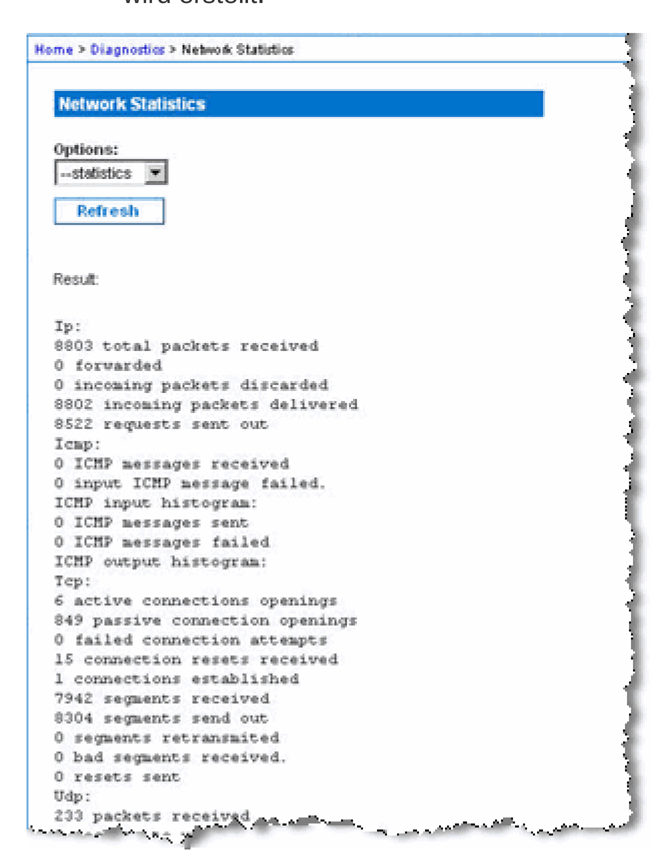
Seite "Network Statistics" (Netzwerkstatistik)

Dominion KX II liefert Statistiken über die Netzwerkschnittstelle.

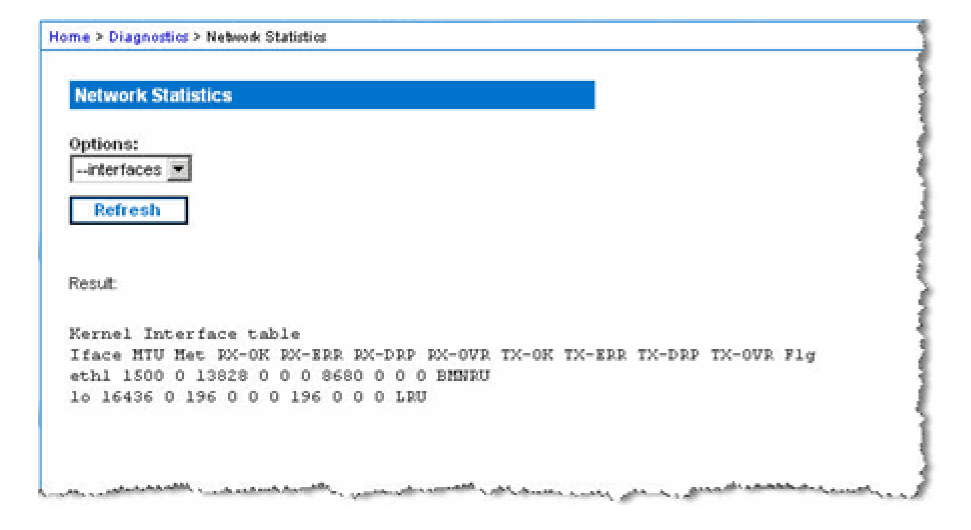
► **So zeigen Sie Statistiken über die Netzwerkschnittstelle an:**

1. Wählen Sie "Diagnostics" > "Network Statistics" (Diagnose > Netzwerkstatistik) aus. Die Seite "Network Statistics" (Netzwerkstatistik) wird angezeigt.
2. Wählen Sie eine Option aus der Dropdownliste "Options":

- Statistics (Statistiken) – Eine Seite, die der hier gezeigten ähnelt, wird erstellt.

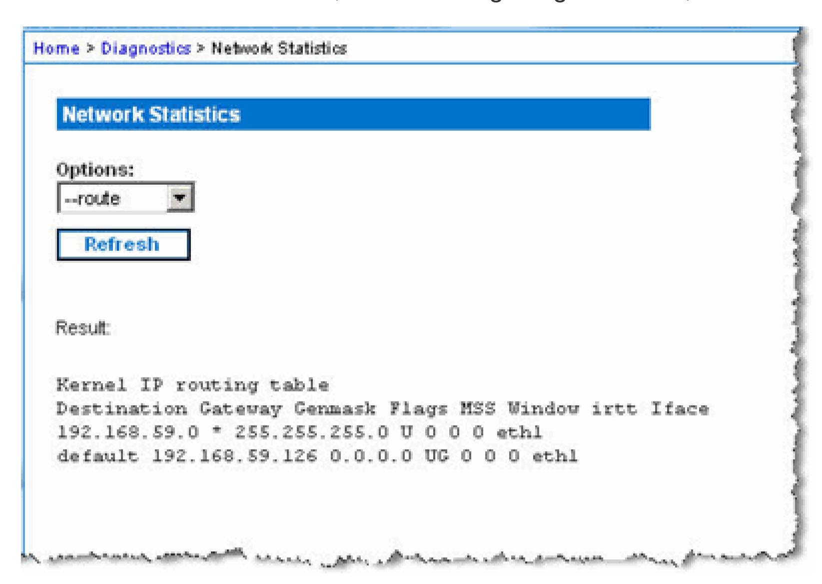


- Interfaces (Schnittstellen) – Eine Seite, die der hier gezeigten ähnelt, wird erstellt.





- Route – Eine Seite, die der hier gezeigten ähnelt, wird erstellt.



3. Klicken Sie auf "Refresh" (Aktualisieren). Die entsprechenden Informationen werden im Feld "Result" (Ergebnis) angezeigt.

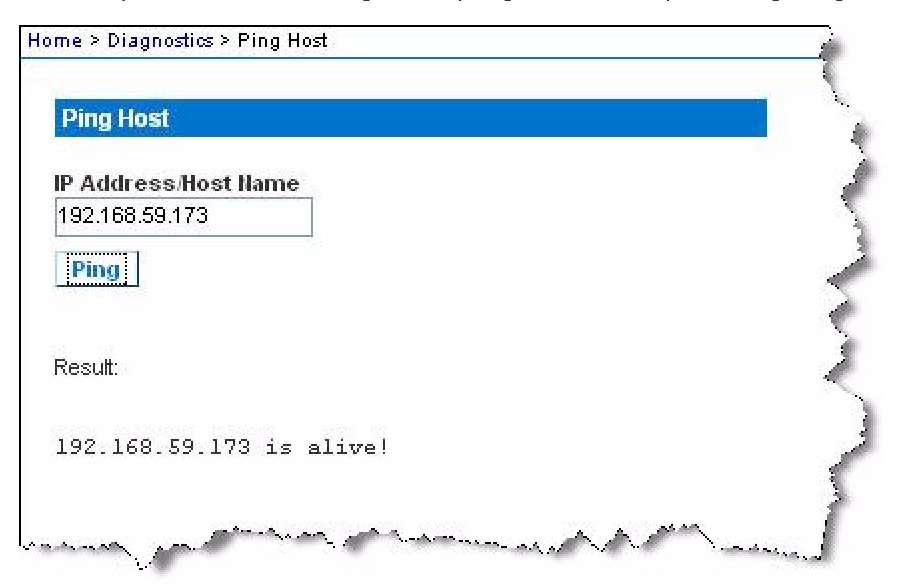


Seite "Ping Host" (Ping an den Host)

Ping ist ein Netzwerktool, mit dem getestet werden kann, ob ein bestimmter Host oder eine IP-Adresse über ein IP-Netzwerk erreichbar ist. Mithilfe der Seite "Ping Host" (Ping an den Host) können Sie herausfinden, ob ein Zielserver oder eine andere Dominion KX II-Einheit erreichbar ist.

So senden Sie ein Ping an den Host:

1. Wählen Sie "Diagnostics" > "Ping Host" (Diagnose > Ping an den Host) aus. Die Seite "Ping Host" (Ping an den Host) wird angezeigt.



2. Geben Sie entweder den Hostnamen oder die IP-Adresse im Feld "IP Address/Host Name" (IP-Adresse/Hostname) ein.

Hinweis: Der Hostname darf aus maximal 232 Zeichen bestehen.

3. Klicken Sie auf "Ping". Die Ping-Ergebnisse werden im Feld "Result" (Ergebnis) angezeigt.

Hinweis: Sowohl IPv4- als auch IPv6-Adressen werden unterstützt.

Seite "Trace Route to Host" (Route zum Host zurückverfolgen)

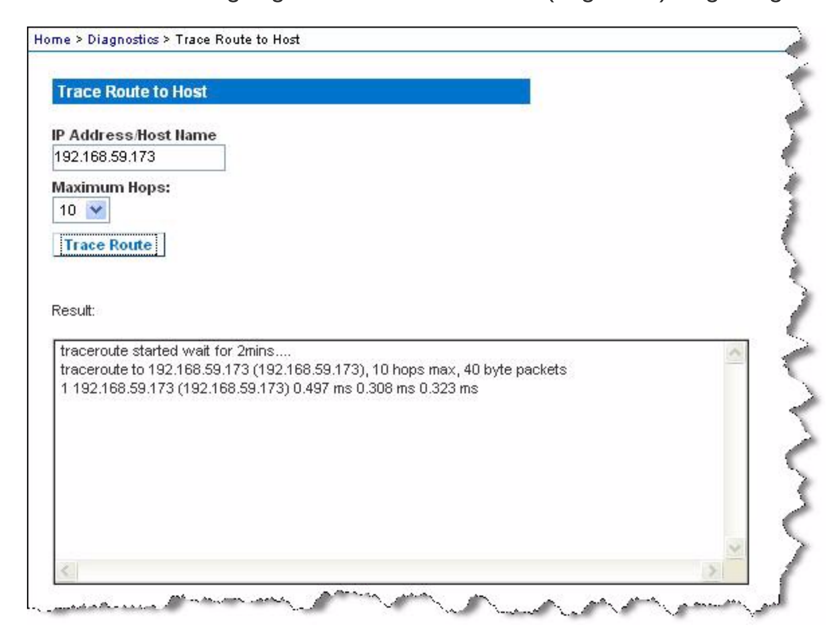
Die Routenverfolgung ist ein Netzwerktool, mit dem Sie die Route bis zum angegebenen Hostnamen oder der IP-Adresse zurückverfolgen können.

So verfolgen Sie die Route bis zum Host zurück:

1. Wählen Sie "Diagnostics" > "Trace Route to Host" (Diagnose > Route zum Host zurückverfolgen) aus. Die Seite "Trace Route to Host" (Route zum Host zurückverfolgen) wird angezeigt.
2. Geben Sie entweder die IP-Adresse oder den Hostnamen im Feld "IP Address/Host Name" (IP-Adresse/Hostname) ein.

   Hinweis: Der Hostname darf aus maximal 232 Zeichen bestehen.

3. Wählen Sie in der Dropdownliste "Maximum Hops" (Maximale Teilstrecken) eine Option aus (5 bis 50 in Schritten von 5).
4. Klicken Sie auf "Trace Route" (Route zurückverfolgen). Der Befehl wird für den angegebenen Hostnamen oder die IP-Adresse sowie die maximale Zahl der Teilstrecken ausgeführt. Das Ergebnis der Routenverfolgung wird im Feld "Result" (Ergebnis) angezeigt.





Device Diagnostics (Gerätediagnose)

Hinweis: Diese Seite ist für die Außendienstmitarbeiter von Raritan gedacht. Verwenden Sie sie nur unter Anleitung des technischen Kundendienstes.

Auf der Seite "Device Diagnostics" (Gerätediagnose) werden die Diagnoseinformationen von Dominion KX II auf den Client-PC heruntergeladen. Auf dieser Seite haben Sie zwei Möglichkeiten:

- Führen Sie während einer Sitzung zum Debuggen eines schwerwiegenden Fehlers ein vom technischen Kundendienst von Raritan bereitgestelltes Spezialdiagnoseskript aus. Das Skript wird auf das Gerät hochgeladen und ausgeführt. Nachdem das Skript ausgeführt wurde, können Sie die Diagnosemeldungen über die Schaltfläche "Save to File" (Speichern unter) herunterladen.
- Laden Sie das Protokoll der Gerätediagnose vom Dominion KX II-Gerät auf den Client herunter, um eine Übersicht der Diagnosemeldungen zu erhalten. Diese verschlüsselte Datei wird anschließend an den technischen Kundendienst von Raritan gesendet. Nur Raritan kann diese Datei interpretieren.

Hinweis: Auf diese Seite können nur Benutzer mit Administratorrechten zugreifen.

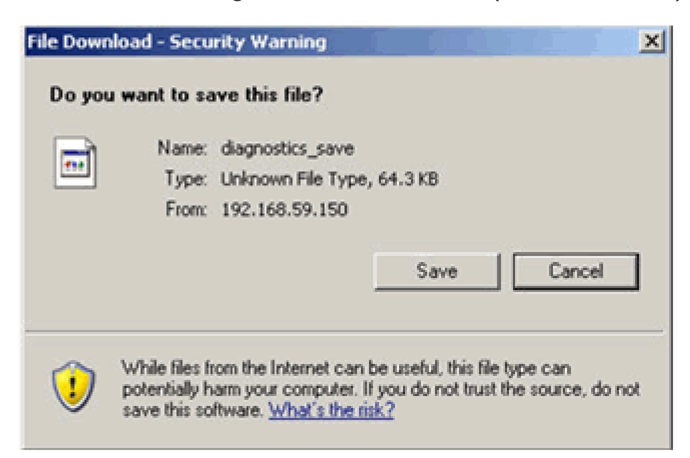
So führen Sie die Dominion KX II-Systemdiagnose aus:

1. Wählen Sie "Diagnostics" > "Dominion KX II Diagnostics" (Diagnose > Dominion KX II-Diagnose) aus. Die Dominion KX II-Diagnoseseite wird angezeigt.
2. So führen Sie eine Diagnoseskriptdatei aus, die Sie per E-Mail vom technischen Kundendienst von Raritan erhalten haben:
   a. Rufen Sie die Diagnosedatei von Raritan ab, und entpacken Sie sie gegebenenfalls.
   b. Klicken Sie auf die Schaltfläche "Browse" (Durchsuchen). Das Dialogfeld "Choose File" (Datei auswählen) wird angezeigt.
   c. Navigieren Sie zur gewünschten Diagnosedatei, und markieren Sie sie.
   d. Klicken Sie auf "Open" (Öffnen). Die Datei wird im Feld "Script File" (Skriptdatei) angezeigt.



   e. Klicken Sie auf "Run Script" (Skript ausführen). Senden Sie diese Datei an den technischen Kundendienst von Raritan.

3. So erstellen Sie eine Diagnosedatei, die Sie an den technischen Kundendienst von Raritan senden können:
   a. Klicken Sie auf die Schaltfläche "Save to File" (Speichern unter). Das Dialogfeld "File Download" (Dateidownload) wird angezeigt.



   b. Klicken Sie auf "Save" (Speichern). Das Dialogfeld "Save As" (Speichern unter) wird angezeigt.
   c. Navigieren Sie zum gewünschten Verzeichnis, und klicken Sie auf "Save" (Speichern).
   d. Senden Sie diese Datei an die vom technischen Kundendienst von Raritan angegebene E-Mail-Adresse.



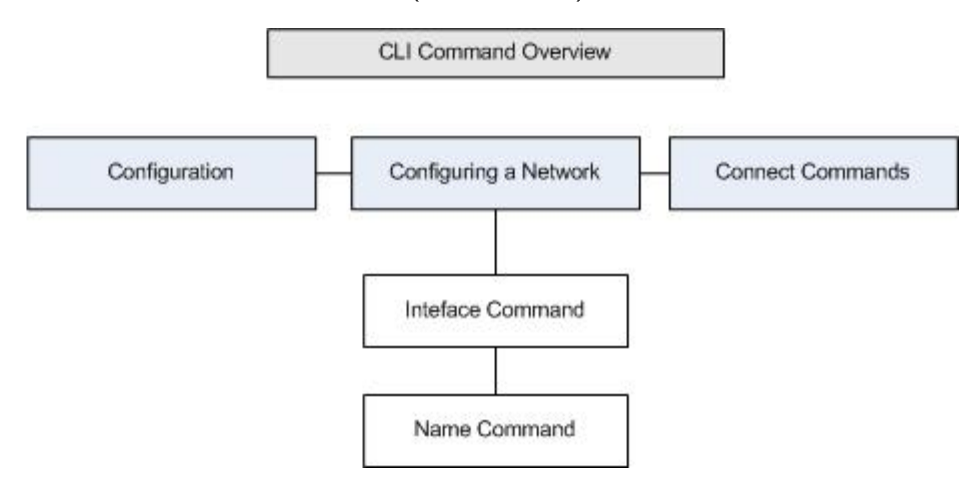
Kapitel 12 Kommandozeilenschnittstelle (CLI)

In diesem Kapitel

Überblick

Die Kommandozeilenschnittstelle (Command Line Interface, CLI) kann verwendet werden, um die Dominion KX II-Netzwerkschnittstelle zu konfigurieren und Diagnosefunktionen durchzuführen, vorausgesetzt, Sie verfügen über die erforderlichen Berechtigungen.

Das folgenden Abbildungen bieten eine Übersicht über die Befehle der Kommandozeilenschnittstelle. Eine Liste der Befehle, einschließlich Definitionen und Verknüpfungen zu den Abschnitten in diesem Kapitel, die Beispiele für diese Befehle enthalten, finden Sie unter ***Befehle der Kommandozeilenschnittstelle*** (auf Seite 281).



Die folgenden allgemeinen Befehle können auf allen Ebenen der Kommandozeilenschnittstelle der Abbildung oben verwendet werden: "top", "history", "log off", "quit", "show" und "help"

Hinweis: Sowohl IPv4- als auch IPv6-Adressen werden unterstützt.

Zugriff auf Dominion KX II über die Kommandozeilenschnittstelle

Verwenden Sie eine der folgenden Methoden, um auf Dominion KX II zuzugreifen:

- Telnet via IP Connection (Telnet über IP-Verbindung)
- SSH (Secure Shell) via IP Connection [SSH (Secure Shell) über IP-Verbindung]
- Local Port-via RS-232 Serial Interface (Lokaler Port über serielle Schnittstelle RS-232)

Verschiedene SSH/Telnet-Clients stehen hier zur Verfügung:

- Putty – ***http://www.chiark.greenend.org.uk/~sgtatham/putty/ http://www.chiark.greenend.org.uk/~sgtatham/putty/***
- SSH Client von ssh.com – ***www.ssh.com http://www.ssh.com***
- Applet SSH Client – ***www.netspace.org/ssh http://www.netspace.org/ssh***
- OpenSSH Client – ***www.openssh.org http://www.openssh.org***

SSH-Verbindung mit Dominion KX II

Verwenden Sie zur Verbindung mit Dominion KX II einen SSH-Client, der SSH V2 unterstützt. Sie müssen den SSH-Zugriff auf der Seite "Devices Services" (Gerätedienste) aktivieren.

Hinweis: Aus Sicherheitsgründen werden SSH-V1-Verbindungen von Dominion KX II nicht unterstützt.

SSH-Zugriff über einen Windows-PC

So öffnen Sie eine SSH-Sitzung über einen Windows®-PC:

1. Starten Sie die SSH-Clientsoftware.
2. Geben Sie die IP-Adresse des Dominion KX II-Servers ein. Beispielsweise 192.168.0.192.
3. Wählen Sie "SSH" aus (der standardmäßige Konfigurations-Port lautet 22).
4. Klicken Sie auf "Open" (Öffnen).



Die Eingabeaufforderung `login as:` (Anmelden als:) wird angezeigt.

Siehe ***Anmelden*** (auf Seite 276).

Hinweis: Sowohl IPv4- als auch IPv6-Adressen werden unterstützt.

SSH-Zugriff über eine UNIX-/Linux-Workstation

Geben Sie den folgenden Befehl ein, um eine SSH-Sitzung über eine UNIX®-/Linux®-Workstation zu öffnen und sich als Admin-Benutzer anzumelden:

```
ssh -l admin 192.168.30.222
```

Die Eingabeaufforderung für das Kennwort wird angezeigt.

Siehe ***Anmelden*** (auf Seite 276).

Hinweis: Sowohl IPv4- als auch IPv6-Adressen werden unterstützt.

Telnet-Verbindung mit Dominion KX II

Aufgrund ungenügender Sicherheit werden Benutzername, Kennwort sowie der gesamte Datenverkehr im Netz verschlüsselt. Der Telnet-Zugriff ist standardmäßig deaktiviert.

Aktivieren von Telnet

Wenn Sie Telnet für den Zugriff auf Dominion KX II verwenden möchten, greifen Sie zuerst über die Kommandozeilenschnittstelle oder einen Browser auf Dominion KX II zu.

So aktivieren Sie Telnet:

- Aktivieren Sie den Telnet-Zugriff im Menü "Device Settings" > "Device Services" (Geräteeinstellungen > Gerätedienste).

Wenn der Telnet-Zugriff aktiviert ist, können Sie über diesen auf Dominion KX II zugreifen und die verbleibenden Parameter einstellen.

Zugriff auf Telnet über einen Windows-PC

So öffnen Sie eine Telnet-Sitzung über einen Windows®-PC:

1. Wählen Sie "Start" > "Ausführen" aus.
2. Geben Sie in das Textfeld "Öffnen" *Telnet* ein.
3. Klicken Sie auf OK. Die Seite "Telnet" wird angezeigt.
4. Wenn Sie dazu aufgefordert werden, geben Sie den folgenden Befehl ein: `Microsoft Telnet> open <IP address>`, wobei <IP address> die IP-Adresse von Dominion KX II ist.

5. Drücken Sie die Eingabetaste. Die folgende Meldung wird angezeigt: `Connecting To <IP address>... (Verbindung zu IP-Adresse wird hergestellt) Die Eingabeaufforderung "login as"` (Anmelden als) wird angezeigt.

Siehe ***Anmelden*** (auf Seite 276).

Hinweis: Sowohl IPv4- als auch IPv6-Adressen werden unterstützt.

Anmelden

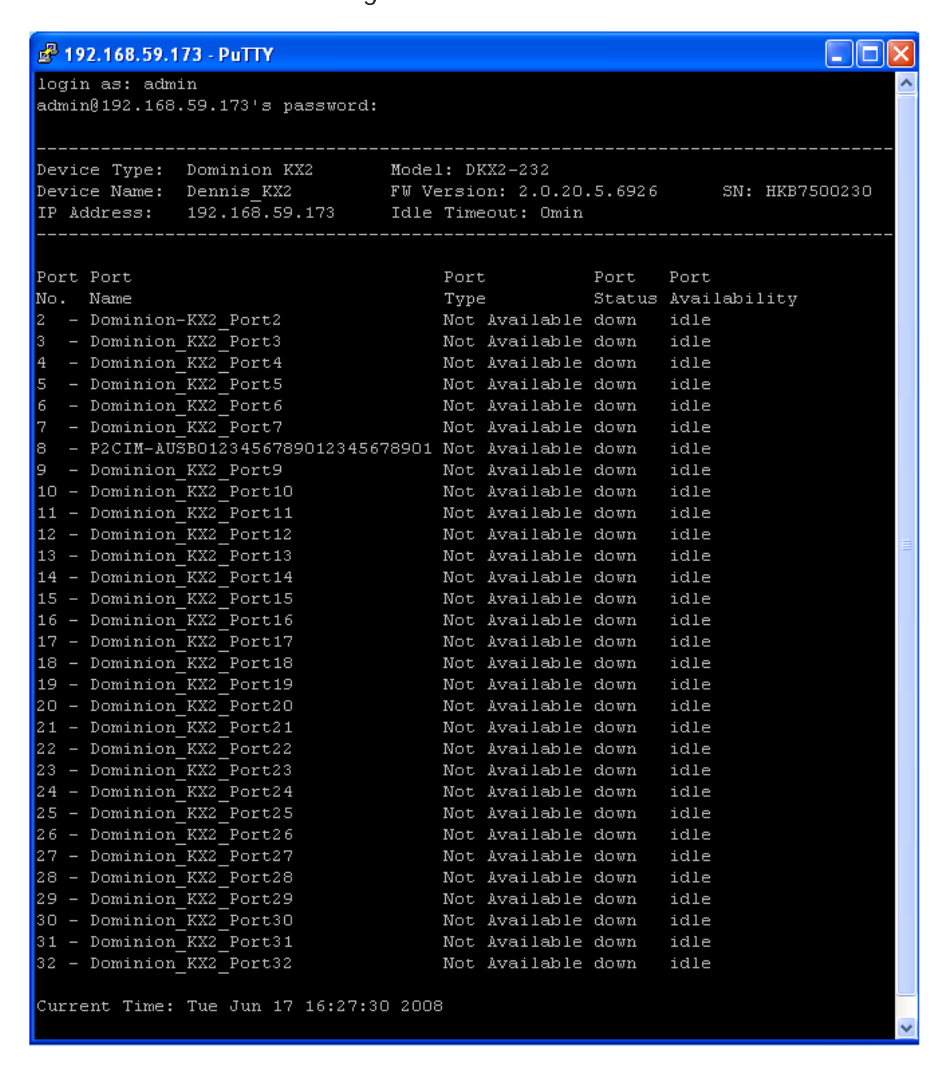
Geben Sie zum Anmelden den Benutzernamen „admin“ wie gezeigt ein:

1. Melden Sie sich als `admin` an.
2. Die Eingabeaufforderung für das Kennwort wird angezeigt. Geben Sie das Standardkennwort ein: *raritan*

   Der Begrüßungsbildschirm wird angezeigt. Sie sind jetzt als Administrator angemeldet.



Wenn Sie den folgenden Abschnitt ***Navigation in der Kommandozeilenschnittstelle*** (auf Seite 277) gelesen haben, können Sie die Schritte zur Erstkonfiguration durchführen.



Navigation in der Kommandozeilenschnittstelle

Vor der Verwendung der Kommandozeilenschnittstelle sollten Sie sich mit der Navigation und Syntax in der Kommandozeilenschnittstelle vertraut machen. Es stehen Ihnen außerdem einige Tastenkombinationen zur Verfügung, mit denen die Verwendung der Kommandozeilenschnittstelle erleichtert wird.

Vervollständigen von Befehlen

Die Kommandozeilenschnittstelle unterstützt das Vervollständigen teilweise eingegebener Befehle. Drücken Sie die Tabulatortaste, wenn Sie die ersten Zeichen eines Eintrags eingegeben haben. Wenn die Zeichen mit einem Befehl eindeutig übereinstimmen, vervollständigt die Kommandozeilenschnittstelle den Eintrag.

- Wird keine Übereinstimmung gefunden, zeigt die Kommandozeilenschnittstelle die gültigen Einträge für die Ebene an.
- Wenn mehrere Übereinstimmungen gefunden werden, zeigt die Kommandozeilenschnittstelle alle gültigen Einträge an.

Geben Sie weiteren Text ein, damit eine eindeutige Übereinstimmung gefunden werden kann, und vervollständigen Sie den Eintrag mithilfe der Tabulatortaste.

Syntax der Kommandozeilenschnittstelle – Tipps und Zugriffstasten

Tipps

- Befehle werden in alphabetischer Reihenfolge aufgeführt.
- Bei Befehlen wird die Groß-/Kleinschreibung nicht beachtet.
- Parameternamen bestehen aus einem Wort ohne Unterstrich.
- Für Befehle ohne Argumente werden standardmäßig die aktuellen Einstellungen für den Befehl angezeigt.
- Wenn Sie nach dem Befehl ein Fragezeichen (?) eingeben, wird die Hilfe für diesen Befehl angezeigt.
- Ein senkrechter Strich (|) zeigt eine Auswahl im Bereich der optionalen oder erforderlichen Schlüsselwörter oder Argumente an.

Zugriffstasten

- Drücken Sie die Pfeil-nach-oben-Taste, um den letzten Eintrag anzuzeigen.
- Drücken Sie die Rücktaste, um das zuletzt eingegebene Zeichen zu löschen.
- Drücken Sie "Strg+C", um einen Befehl zu beenden oder abzubrechen, wenn Sie die falschen Parameter eingegeben haben.
- Drücken Sie die Eingabetaste, um den Befehl auszuführen.
- Drücken Sie die Tabulatortaste, um einen Befehl zu vervollständigen. Beispiel: `Admin Port > Conf.` Das System zeigt dann die Eingabeaufforderung `Admin Port > Config >` an.



Allgemeine Befehle für alle Ebenen der Kommandozeilenschnittstelle

Im Folgenden werden die Befehle aufgelistet, die auf allen Ebenen der Kommandozeilenschnittstelle verfügbar sind. Diese Befehle dienen auch zur Navigation in der Kommandozeilenschnittstelle.

Befehle	Beschreibung
top	Wechselt zur höchsten Ebene der Hierarchie der Kommandozeilenschnittstelle oder der Eingabeaufforderung "username" (Benutzername).
history	Zeigt die letzten 200 Befehle an, die der Benutzer in die Kommandozeilenschnittstelle von Dominion KX II eingegeben hat.
help	Zeigt eine Übersicht der Syntax der Kommandozeilenschnittstelle an.
quit	Der Benutzer kehrt eine Ebene zurück.
logout	Beendet die Benutzersitzung.

Erstkonfiguration über die Kommandozeilenschnittstelle

Hinweis: Diese Schritte unter Verwendung der Kommandozeilenschnittstelle sind optional, da dieselbe Konfiguration auch über KVM erfolgen kann. Weitere Informationen finden Sie unter **Erste Schritte** *(auf Seite 15).*

Dominion KX II-Geräte werden werksseitig mit Standardeinstellungen geliefert. Wenn Sie das Gerät zum ersten Mal einschalten und verbinden, müssen Sie die folgenden Grundparameter einstellen, sodass vom Netzwerk aus sicher auf das Gerät zugegriffen werden kann.

1. Kennwort des Administrators zurücksetzen. Alle Dominion KX II-Geräte verfügen zunächst über dasselbe Standardkennwort. Um Sicherheitsverletzungen zu vermeiden, müssen Sie deshalb das Administratorkennwort "raritan" in ein benutzerdefiniertes Kennwort für Administratoren, die das Dominion KX II-Gerät verwalten, ändern.
2. IP-Adresse, Subnetzmaske und Gateway-IP-Adresse für Remotezugriff zuweisen.

Hinweis: Sowohl IPv4- als auch IPv6-Adressen werden unterstützt.

Einstellen von Parametern

Um Parameter einzustellen, müssen Sie sich als Administrator anmelden. Auf der höchsten Ebene wird die Eingabeaufforderung "Username" > (Benutzername) angezeigt, der bei der Erstkonfiguration "admin" lautet. Geben Sie den Befehl "top" ein, um zur höchsten Menüebene zurückzukehren.

Hinweis: Wenn Sie sich mit einem anderen Benutzernamen angemeldet haben, wird dieser anstatt "admin" angezeigt.

Einstellen von Netzwerkparametern

Netzwerkparameter werden mithilfe des Befehls "interface" konfiguriert:

```
admin > Config > Network > interface enable true if lan1
ip 192.16.151.12 mask 255.255.255 gw 192.168.51.12
```

Wenn der Befehl akzeptiert wird, trennt das Gerät automatisch die Verbindung. Sie müssen die Verbindung zum Gerät unter Verwendung der neuen IP-Adresse und des Benutzernamens und des Kennworts, die Sie im Abschnitt zum Zurücksetzen des werkseitigen Standardkennworts erstellt haben, erneut herstellen.

Wichtig: Wenn Sie das Kennwort vergessen, muss Dominion KX II über die Taste "Reset" (Zurücksetzen) auf der Rückseite von Dominion KX II auf die Werkseinstellungen zurückgesetzt werden. Die Schritte zur Erstkonfiguration müssen in diesem Fall erneut durchgeführt werden.

Dominion KX II verfügt nun über die Grundkonfiguration, und Sie können von einem Remotestandort aus (SSH oder GUI) sowie lokal mithilfe des lokalen seriellen Ports auf die Einheit zugreifen. Der Administrator muss Benutzer und Gruppen, Dienste, Sicherheit und serielle Ports, über die die seriellen Zielgeräte an Dominion KX II angeschlossen sind, konfigurieren.

Hinweis: Sowohl IPv4- als auch IPv6-Adressen werden unterstützt.

Eingabeaufforderungen der Kommandozeilenschnittstelle

Die Eingabeaufforderung der Kommandozeilenschnittstelle zeigt die aktuelle Befehlsebene an. Die Stammebene der Eingabeaufforderung ist der Anmeldename. Bei einer direkten Verbindung mit dem seriellen Port "Admin" mit einem Terminalemulationsprogramm ist "Admin Port" (Admin-Port) die Stammebene eines Befehls:

```
admin >
```

Bei TELNET/SSH ist "admin" die Stammebene des Befehls:



```
admin > config > network >
```

0

Befehle der Kommandozeilenschnittstelle

- Geben Sie `admin > help` ein.

Befehl	Beschreibung
config	Wechselt zum Konfigurationsuntermenü.
diagnostics	Wechselt zum Diagnoseuntermenü.
help	Zeigt einen Überblick der Befehle an.
history	Zeigt den Kommandozeilenverlauf der aktuellen Sitzung an.
listports	Listet die verfügbaren Ports auf.
logout	Abmeldung von der aktuellen Sitzung der Kommandozeilenschnittstelle
top	Kehrt zum Stammmenü zurück.
userlist	Listet aktive Benutzersitzungen auf.

- Geben Sie "admin > config > network" ein.

Befehl	Beschreibung
help	Zeigt einen Überblick der Befehle an.
history	Zeigt den Kommandozeilenverlauf der aktuellen Sitzung an.
interface	Einstellen/Empfangen von Netzwerkparametern
ipv6_interface	Einstellen/Empfangen von IPv6-Netzwerkparametern
logout	Abmeldung von der aktuellen Sitzung der Kommandozeilenschnittstelle
name	Gerätenamenkonfiguration
quit	Kehrt zum vorherigen Menü zurück.
stop	Kehrt zum Stammmenü zurück.

Sicherheitsprobleme

Wichtige Elemente, die Sie bei der Sicherheit für Konsolenserver beachten sollten:

- Verschlüsselung des Datenverkehrs zwischen Bedienerkonsole und dem Dominion KX II-Gerät
- Authentifizierung und Autorisierung von Benutzern
- Sicherheitsprofil

Dominion KX II unterstützt diese drei Elemente. Sie müssen jedoch vor dem Gebrauch konfiguriert werden.

Verwalten der Befehle für die Konsolenserverkonfiguration von Dominion KX II

Hinweis: Die Befehle der Kommandozeilenschnittstelle bleiben für SSH-, Telnet- und lokale Portzugriffssitzungen gleich.

Auf den Netzwerkbefehl kann über das Menü "Configuration" (Konfiguration) des Dominion KX II zugegriffen werden.

Konfigurieren des Netzwerks

Die Netzwerkmenübefehle werden verwendet, um den Dominion KX II-Netzwerkadapter zu konfigurieren.

Befehle	Beschreibung
interface	Konfiguriert die Netzwerkschnittstelle des Dominion KX II-Geräts.
name	Netzwerknamenkonfiguration
ipv6	Einstellen/Empfangen von IPv6-Netzwerkparametern



Befehl "interface"

Der Befehl "interface" wird zur Konfiguration der Netzwerkschnittstelle des Dominion KX II verwendet. Verwenden Sie folgende Syntax für den Befehl "interface":

```
interface [ipauto <none|dhcp>] [ip <ipaddress>] [mask <subnetmask>] [gw <ipaddress>] [mode <mode>]

Einstellen/Empfangen von Ethernet-Parametern

ipauto <none|dhcp> IP auto configuration (none/dhcp)

ip <ipaddress> IP Address

mask <subnetmask> Subnet Mask

gw <ipaddress> Gateway IP Address

mode <mode> Set Ehternet Mode (auto/10hdx/10fdx/100hdx/100fdx/1000fdx)
```

Beispiel für den Befehl "interface"

Der folgende Befehl aktiviert die Schnittstelle Nr. 1, legt die IP-Adresse, Maske und Gateway-Adressen sowie den Modus auf automatische Erkennung fest.

```
Admin > Config > Network > interface ipauto none ip 192.16.151.12 mask 255.255.255.0 gw 192.168.51.12 mode auto
```

Hinweis: Sowohl IPv4- als auch IPv6-Adressen werden unterstützt.

Befehl "name"

Der Befehl "name" wird zur Konfiguration des Netzwerknamens verwendet. Verwenden Sie folgende Syntax für den Namen:

```
name [devicename <devicename>] [hostname <hostname>]
```

Gerätenamenkonfiguration

```
devicename <devicename>   Device Name

hostname   <hostname>    Preferred host name (DHCP only)
```

Beispiel für den Befehl "name"

Folgender Befehl legt den Netzwerknamen fest:

```
Admin > Config > Network > name devicename My-KSX2
```



Befehl "IPv6"

Verwenden Sie den Befehl "IPv6", um die IPv6-Netzwerkparameter festzulegen und bestehende IPv6-Parameter abzurufen.



Kapitel 13 Lokale Dominion KX II-Konsole

In diesem Kapitel

Überblick

Sie können am Serverschrank über den lokalen Port auf Dominion KX II zugreifen und die Einheit verwalten. Dieser lokale Port bietet eine browserbasierte grafische Benutzeroberfläche, mit der Sie schnell und komfortabel zwischen den Servern wechseln können. Die lokale Dominion KX II-Konsole stellt eine direkte analoge Verbindung mit den angeschlossenen Servern her. Die Leistung ist mit der Leistung bei einer direkten Verbindung mit der Tastatur, der Maus und den Videoports des Servers identisch. Die lokale Dominion KX II-Konsole bietet dieselben Verwaltungsfunktionen wie die Dominion KX II-Remotekonsole.

Verwenden der lokalen Dominion KX II-Konsole

Gleichzeitige Benutzer

Die lokale Dominion KX II-Konsole stellt einen unabhängigen Zugriffspfad zu den angeschlossenen KVM-Zielservern bereit. Die Verwendung der lokalen Konsole hindert andere Benutzer nicht daran, gleichzeitig eine Netzwerkverbindung herzustellen. Auch wenn Remotebenutzer mit Dominion KX II verbunden sind, können Sie gleichzeitig über die lokale Konsole im Serverschrank auf die Server zugreifen.

Oberfläche der lokalen Dominion KX II-Konsole

Am Serverschrank erfüllt Dominion KX II über die lokale Dominion KX II-Konsole standardmäßige KVM-Management- und Verwaltungsfunktionen. Die lokale Dominion KX II-Konsole stellt eine direkte KVM-Verbindung (analog) mit den angeschlossenen Servern her. Die Leistung ist mit der Leistung bei einer direkten Verbindung mit der Tastatur, der Maus und den Videoports des Servers identisch.

Die grafischen Benutzeroberflächen der lokalen Dominion KX II-Konsole und der Dominion KX II-Remotekonsole verfügen über zahlreiche Gemeinsamkeiten. Auf die Unterschiede wird in diesem Hilfedokument hingewiesen.

Die Dominion KX II-Option "Local Console Factory Reset" (Werksrücksetzung der lokalen Konsole) ist bei der lokalen Dominion KX II-Konsole verfügbar, jedoch nicht bei der Dominion KX II-Remotekonsole.

Sicherheit und Authentifizierung

Zur Verwendung der lokalen Dominion KX II-Konsole müssen Sie zunächst mit einem gültigen Benutzernamen und Kennwort authentifiziert werden. Dominion KX II verfügt über ein vollständig integriertes Authentifizierungs- und Sicherheitsschema, unabhängig davon, ob Sie über das Netzwerk oder den lokalen Port auf das Gerät zugreifen. In jedem Fall ermöglicht Dominion KX II den Zugriff nur auf die Server, für die ein Benutzer über eine Zugriffsberechtigung verfügt. Weitere Informationen zum Festlegen des Serverzugriffs und der Sicherheitseinstellungen finden Sie unter ***Benutzerverwaltung*** (siehe "***User Management (Benutzerverwaltung)***" auf Seite 128).

Wenn Ihr Dominion KX II für externe Authentifizierungsdienste (LDAP/LDAPS, RADIUS oder Active Directory) konfiguriert wurde, werden Authentifizierungsversuche in der lokalen Konsole auch durch den externen Authentifizierungsdienst authentifiziert.

Hinweis: Sie können für den lokalen Konsolenzugriff auch festlegen, dass keine Authentifizierung erfolgen soll. Diese Option wird jedoch nur für sichere Umgebungen empfohlen.

▶ So verwenden Sie die lokale Dominion KX II-Konsole:

1. Schließen Sie an die lokalen Ports auf der Rückseite des Dominion KX II-Geräts eine Tastatur, eine Maus und eine Videoanzeige an.
2. Starten Sie Dominion KX II. Die Oberfläche der lokalen Dominion KX II-Konsole wird angezeigt.



Smart Card-Zugriff von der lokalen Konsole

Um mit einer Smart Card von der lokalen Konsole auf einen Server zuzugreifen, schließen Sie ein Smart Card-USB-Lesegerät an Dominion KX II an. Nutzen Sie dazu einen der USB-Ports am Dominion KX II-Gerät. Sobald ein Smart Card-Lesegerät am Dominion KX II-Gerät ein- oder ausgesteckt wird, wird dies von Dominion KX II automatisch erkannt. Eine Liste der unterstützten Smart Cards und Informationen zu zusätzlichen Systemanforderungen finden Sie unter ***Unterstützte und nicht unterstützte Smart Card-Lesegeräte*** (auf Seite 326) und unter ***Minimale Systemanforderungen*** (siehe "***Mindestanforderungen an das System***" auf Seite 327).

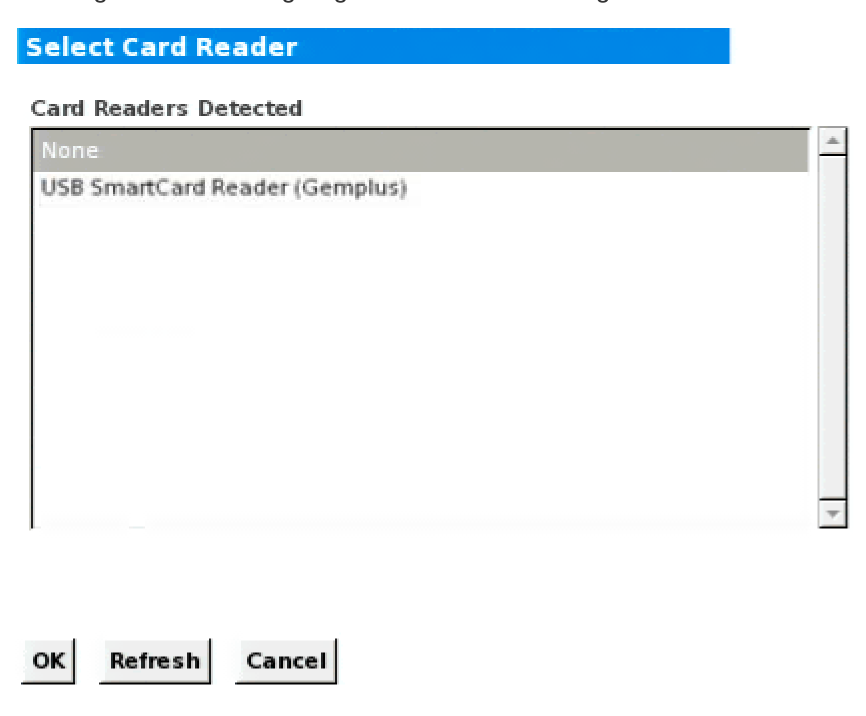
Nach der Installation des Kartenlesegeräts und der Smart Card auf dem Zielserver, funktioniert der Server so, als wären das Kartenlesegerät und die Smart Card direkt am Server angeschlossen. Abhängig von den Einstellungen in den Richtlinien zur Entfernung der Karte im Betriebssystem des Zielservers wird beim Entfernen der Smart Card oder des Smart Card-Lesegeräts die Benutzersitzung gesperrt, oder Sie werden abgemeldet. Ist die KVM-Sitzung unterbrochen, weil Sie beendet wurde oder Sie auf ein neues Ziel umgeschaltet haben, wird das Smart Card-Kartenlesegerät automatisch vom Zielserver deinstalliert.

So mounten Sie ein Smart Card-Lesegerät über die lokale Dominion KX II-Konsole auf einem Ziel.

1. Stecken Sie ein Smart Card-USB-Lesegerät am Dominion KX II-Gerät ein. Nutzen Sie dazu einen der USB-Ports des Geräts. Sobald das Smart Card-Lesegerät angeschlossen ist, wird es von Dominion KX II erkannt.
2. Klicken Sie in der lokalen Konsole auf "Tools" (Extras).
3. Wählen Sie in der Liste "Card Readers Detected" (Erkannte Smart Card-Lesegeräte) das Smart Card-Lesegerät aus. Wählen Sie in der Liste die Option "None" (Keines) aus, wenn Sie keines der Lesegeräte mounten möchten.
4. Klicken Sie auf OK. Sobald das Smart Card-Lesegerät hinzugefügt wurde, wird auf der Seite eine Meldung angezeigt, die Sie darauf hinweist, dass der Vorgang erfolgreich abgeschlossen wurde. Der jeweilige Status "Selected" (Ausgewählt) oder "Not Selected" (Nicht ausgewählt) wird im linken Fenster der Seite unter "Card Reader" (Smart Card-Lesegerät) angezeigt.

So aktualisieren Sie die Liste "Card Readers Detected" (Erkannte Smart Card-Lesegeräte):

- Klicken Sie auf "Refresh" (Aktualisieren), wenn ein neues Smart Card-Lesegerät gemounted wurde. Die Liste "Card Readers Detected" (Erkannte Smart Card-Lesegeräte) wird aktualisiert und zeigt die neu hinzugefügten Smart Card-Lesegeräte an.



Smart Card-Zugriff bei KX2 8-Geräten

Wenn Sie ein Smart Card-Lesegerät verwenden, um von der lokalen Konsole über ein KX2-832- oder KX2-864-Gerät auf einen Server zuzugreifen, muss der erweiterte lokale Port (Seite "Local Port Settings" [Lokale Porteinstellungen]) deaktiviert sein. Der erweiterte lokale Port unterstützt keine Smart Card-Authentifizierung.



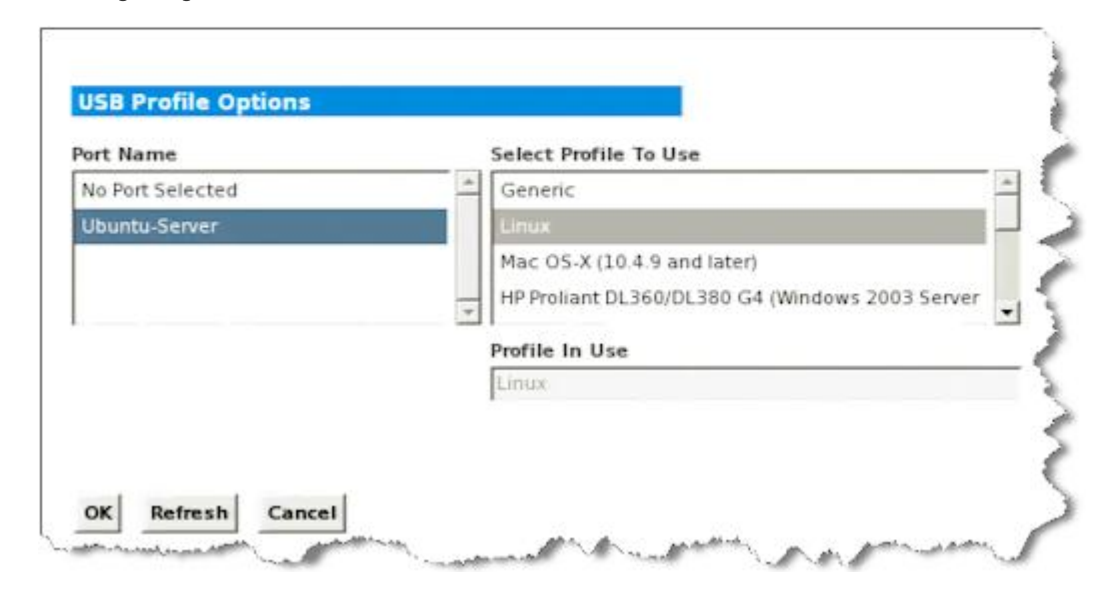
USB-Profiloptionen der lokalen Konsole

Wählen Sie im Abschnitt "USB Profile Options" (USB-Profiloptionen) auf der Seite "Tools" (Extras) ein verfügbares USB-Profil für einen lokalen Port aus.

Die Ports, die Profilen zugewiesen werden können, werden im Feld "Port Name" angezeigt, und die für einen Port verfügbaren Profile werden im Feld "Select Profile To Use" (Zu verwendendes Profil auswählen) angezeigt, nachdem der Port ausgewählt wurde. Die Profile, die für die Verwendung mit einem Port ausgewählt wurden, werden im Feld "Profile In Use" (Verwendetes Profil) angezeigt.

▶ So weisen Sie einem Port der lokalen Konsole ein USB-Profil hinzu:

1. Wählen Sie im Feld "Port Name" den Port aus, den Sie dem USB-Profil zuweisen möchten.
2. Wählen Sie im Feld "Select Profile To Use" (Zu verwendendes Profil auswählen) das gewünschte Profil aus den für den Port verfügbaren Profilen aus.
3. Klicken Sie auf OK. Das USB-Profil wird für den lokalen Port übernommen und im Feld "Profile In Use" (Verwendetes Profil) angezeigt.



Verfügbare Auflösungen

Die lokale Dominion KX II-Konsole bietet folgende Auflösungen, um verschiedene Monitore zu unterstützen:

- 800 x 600
- 1024 x 768
- 1280 x 1024

Alle Auflösungen unterstützen eine Aktualisierungsfrequenz von 60 Hz und 75 Hz.



Seite "Port Access" (Portzugriff) (Anzeige des lokalen Konsolenservers)

Nachdem Sie sich bei der lokalen Dominion KX II-Konsole angemeldet haben, wird die Seite "Port Access" (Portzugriff) angezeigt. Diese Seite enthält alle Dominion KX II-Ports, die angeschlossenen KVM-Zielserver sowie deren Status und Verfügbarkeit.

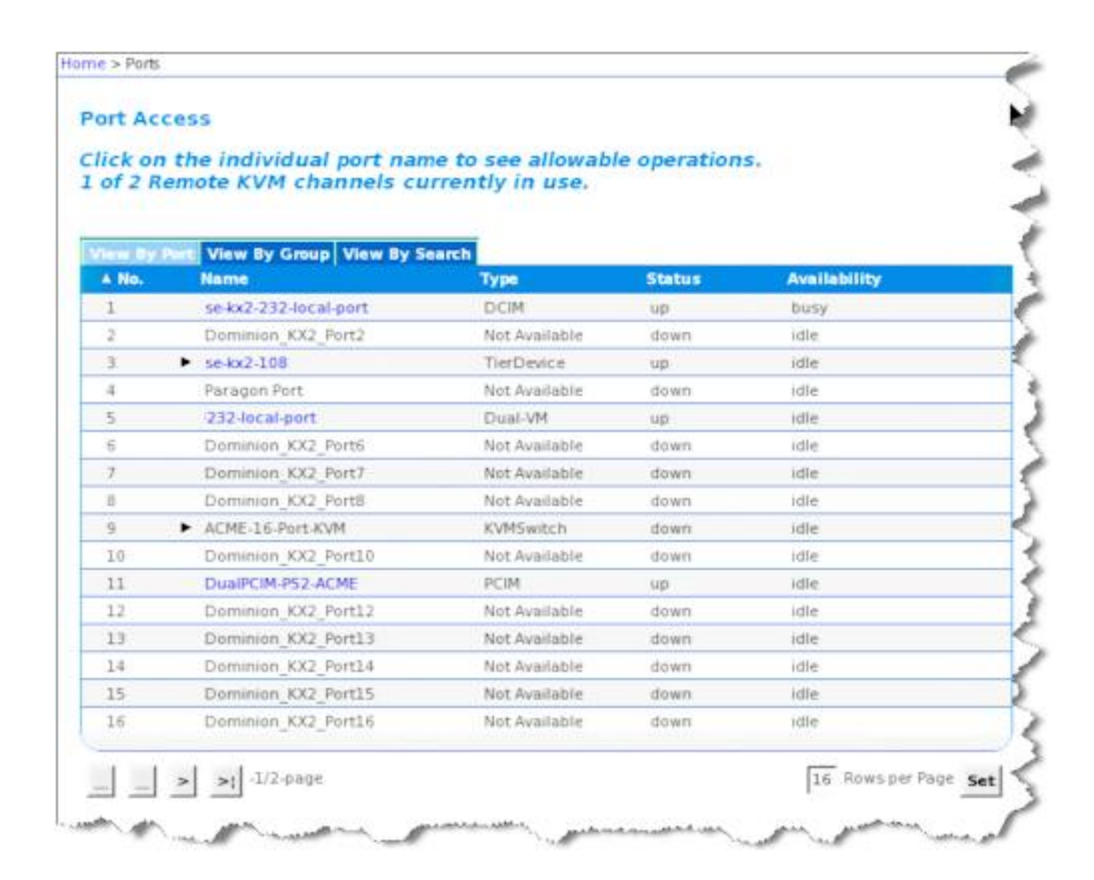
Auf der Seite "Port Access" (Portzugriff) werden außerdem Blade-Chassis angezeigt, die im Dominion KX II konfiguriert wurden. Das Blade-Chassis wird in einer erweiterbaren, hierarchischen Liste auf der Seite "Port Access" (Portzugriff) angezeigt, wobei das Blade-Chassis auf Stammebene der Hierarchie angezeigt und die einzelnen Blades unterhalb der Stammebene bezeichnet und angezeigt werden. Verwenden Sie das Symbol "Expand Arrow" (Pfeil erweitern) neben dem Stamm-Chassis, um die einzelnen Blades anzuzeigen.

Hinweis: Um das Blade-Chassis in hierarchischer Reihenfolge anzuzeigen, müssen für das Bladeserver-Chassis Blade-Chassis-Subtypen konfiguriert werden.

Wenn Sie eine Schichtkonfiguration verwenden, in der ein Dominion KX II-Basisgerät für den Zugriff auf mehrere andere Schichtgeräte verwendet wird, werden die Schichtgeräte auf der Seite "Port Access" (Portzugriff) angezeigt, wenn Sie auf das Symbol "Expand Arrow" (Pfeil erweitern) ► links neben dem Basisgerätenamen klicken. Weitere Informationen zu Schichten finden Sie unter ***Konfigurieren und Aktivieren von Schichten*** (auf Seite 167).

Standardmäßig wird die Registerkarte "View by Port" (Ansicht nach Port) auf der Seite "Port Access" (Portzugriff) angezeigt. Auf der Registerkarte "View by Group" (Ansicht nach Gruppe) werden Portgruppen angezeigt. Die Registerkarte kann erweitert werden, um die der Portgruppe zugewiesenen Ports anzuzeigen. Mithilfe der Registerkarte "View by Search" (Ansicht nach Suche) können Sie nach Portnamen suchen. Die Suchfunktion unterstützt die Verwendung eines Sternchens (*) als Platzhalter sowie die Verwendung vollständiger Namen und Teile von Namen.





So verwenden Sie die Seite "Port Access" (Portzugriff):

1. Melden Sie sich an der lokalen Konsole an.

   Die KVM-Zielserver werden zuerst nach Portnummer sortiert. Sie können die Anzeige so ändern, dass nach einer beliebigen Spalte sortiert wird.

   - Port Number (Portnummer) – Die für das Dominion KX II-Gerät verfügbaren Ports werden beginnend mit 1 durchnummeriert. Beachten Sie, dass mit Powerstrips verbundene Ports hier nicht aufgeführt werden, was zu Lücken in der Portnummernabfolge führt.
   - Port Name (Portname) – Der Name des Dominion KX II-Ports. Standardmäßig lautet dieser "Dominion-KX2-Port#", Sie können den Namen jedoch durch einen aussagekräftigeren ersetzen. Wenn Sie auf einen Portnamenlink klicken, wird das Menü "Port Action" (Portaktion) geöffnet.

   Hinweis: Verwenden Sie für den Port (CIM)-Namen keine Auslassungszeichen (Apostroph).

   - Status – Der Status für Standardserver lautet entweder "Up" (Ein) oder "Down" (Aus).



- Type (Typ) – Der Server- oder CIM-Typ. Bei Blade-Chassis kann der Typ "Blade Chassis", "Blade", "BladeChassisAdmin" oder "BladeChassisURL" lauten. Der Typ kann auch "TierDevice" und "KVMSwitch" enthalten.
- Availability (Verfügbarkeit) – Für die Verfügbarkeit stehen die Werte Idle (Inaktiv), Connected (Verbunden), Busy (Verwendet) und Unavailable (Nicht verfügbar) zur Verfügung. Die Verfügbarkeit der Bladeserver lautet entweder "Shared" (Freigegeben) oder "Exclusive" (Exklusiv), wenn eine Verbindung zu diesem Blade besteht.

2. Klicken Sie auf "View by Port" (Ansicht nach Port) oder auf "View by Group" (Ansicht nach Gruppe), um zwischen den Ansichten zu wechseln.
   - Zusätzlich zu "Port Number" (Portnummer), "Port Name" (Portname), Status, "Type" (Typ) und "Availability" (Verfügbarkeit) wird auf der Registerkarte "View by Group" (Ansicht nach Gruppe) auch eine Gruppenspalte angezeigt. Diese Spalte enthält die verfügbaren Portgruppen.
3. Klicken Sie auf den Portnamen des Zielservers, auf den Sie zugreifen möchten. Das Menü "Port Action" (Portaktion) wird angezeigt. Informationen zu verfügbaren Menüoptionen finden Sie unter **Menü "Port Action" (Portaktion)** (auf Seite 52).
4. Wählen Sie im Menü "Port Action" (Portaktion) den gewünschten Menübefehl aus.

So ändern Sie die Sortierreihenfolge der Anzeige:

- Klicken Sie auf die Spaltenüberschrift, nach der sortiert werden soll. Die Liste der KVM-Zielserver wird nach dieser Spalte sortiert.

Zugriffstasten und Verbindungstasten

Da die Oberfläche der lokalen Dominion KX II-Konsole vollständig durch die Oberfläche des Zielservers ersetzt wird, auf den Sie zugreifen, wird eine Zugriffstaste verwendet, um die Verbindung zu einem Ziel zu trennen und zur GUI des lokalen Ports zurückzukehren. Um eine Verbindung zu einem Ziel herzustellen oder zwischen Zielen zu wechseln wird eine Verbindungstaste verwendet.

Über die Zugriffstaste für den lokalen Port können Sie schnell die Benutzeroberfläche der lokalen Dominion KX II-Konsole aufrufen, wenn gerade ein Zielserver angezeigt wird. Gemäß der Voreinstellung müssen Sie die Rollen-Taste zweimal kurz hintereinander drücken. Sie können jedoch [auf der Seite "Local Port Settings" (Lokale Porteinstellungen)] eine andere Tastenkombination als Zugriffstaste festlegen. Weitere Informationen finden Sie unter Lokale Porteinstellungen für die lokale Dominion KX II-Konsole.

Beispiele für Verbindungstasten

Standardserver	
Funktion der Verbindungstaste	**Beispiel für Tastenfolge**
Auf einen Port über die GUI des lokalen Ports zugreifen	Zugriff auf Port 5 über die GUI des lokalen Ports: • Linke Alt-Taste drücken > Taste "5" drücken und wieder loslassen > Linke Alt-Taste wieder loslassen
Zwischen Ports wechseln	Von Port 5 auf Port 11 wechseln: • Linke Alt-Taste drücken > Taste "1" drücken und wieder loslassen > Taste "1" erneut drücken und wieder loslassen > Linke Alt-Taste wieder loslassen
Verbindung zu einem Zielgerät trennen und zur GUI des lokalen Ports zurückkehren	Verbindung zum Zielport 11 trennen und zur GUI des lokalen Ports zurückkehren (zu der Seite, von der aus Sie eine Verbindung zum Zielgerät hergestellt haben): • Rollen-Taste zweimal drücken

Blade-Chassis	
Funktion der Verbindungstaste	**Beispiel für Tastenfolge**
Auf einen Port über die GUI des lokalen Ports zugreifen	Zugriff auf Port 5, Slot 2: • Linke Alt-Taste drücken > Taste "5" drücken und wieder loslassen > Taste "-" drücken und wieder loslassen > Taste "2" drücken und wieder loslassen > Linke Alt-Taste wieder loslassen
Zwischen Ports wechseln	Von Zielport 5, Slot 2 auf Port 5, Slot 11 wechseln: • Linke Alt-Taste drücken > Taste "5" drücken und wieder loslassen > Taste "-" drücken und wieder loslassen > Taste "1" drücken und wieder loslassen > Taste "1" erneut drücken und wieder loslassen > Linke Alt-Taste wieder loslassen
Verbindung zu einem Zielgerät	Verbindung zum Zielport 5, Slot 11 trennen und zur GUI des lokalen Ports zurückkehren (zu der



Blade-Chassis	
Funktion der Verbindungstaste	**Beispiel für Tastenfolge**
trennen und zur GUI des lokalen Ports zurückkehren	Seite, von der aus Sie eine Verbindung zum Zielgerät hergestellt haben): • Rollen-Taste zweimal drücken

Spezielle Tastenkombinationen für Sun

Die folgenden Tastenkombinationen für spezielle Tasten von Sun Microsystems-Servern sind für den lokalen Port verfügbar. Diese speziellen Tasten sind im Menü "Keyboard" (Tastatur) verfügbar, wenn Sie eine Verbindung zu einem Sun™-Zielserver herstellen.

Sun-Taste	Tastenkombination für lokalen Port
Again	Strg+Alt+F2
Props	Strg+Alt+F3
Undo	Strg+Alt+F4
Stop A	Untbr a
Front	Strg+Alt+F5
Copy	Strg+Alt+F6
Open	Strg+Alt+F7
Find	Strg+Alt+F9
Cut	Strg+Alt+F10
Paste	Strg+Alt+F8
Mute (Stummschaltung)	Strg+Alt+F12
Compose	Strg+Alt+Nummernfeld *
Vol +	Strg+Alt+Nummernfeld +
Vol -	Strg+Alt+Nummernfeld -
Stop	Keine Tastenkombination
Stromversorgung	Keine Tastenkombination

Zugreifen auf einen Zielserver

So greifen Sie auf einen Zielserver zu:

1. Klicken Sie auf den Portnamen des Zielgeräts, auf das Sie zugreifen möchten. Das Menü "Port Action" (Portaktion) wird angezeigt.
2. Wählen Sie im Menü "Port Action" (Portaktion) die Option "Connect" (Verbinden) aus. Die Videoanzeige wechselt zur Oberfläche des Zielservers.

Zurückkehren zur Oberfläche der lokalen Dominion KX II-Konsole

Wichtig: Um über die Standardzugriffstaste auf die lokale Dominion KX II-Konsole zuzugreifen, müssen Sie die Rollen-Taste zweimal kurz hintereinander drücken. Diese Tastenkombination können Sie auf der Seite "Local Port Settings" (Lokale Porteinstellungen) ändern. Siehe Lokale Porteinstellungen für die lokale Dominion KX II-Konsole.

So kehren Sie vom Zielserver zur lokalen Dominion KX II-Konsole zurück:

- Drücken Sie die Zugriffstaste zweimal schnell hintereinander (die Standardzugriffstaste ist die Rollen-Taste). Die Videoanzeige wechselt von der Oberfläche des Zielservers zur Oberfläche der lokalen Dominion KX II-Konsole.

Verwaltung über den lokalen Port

Dominion KX II kann entweder über die lokale Dominion KX II-Konsole oder die Dominion KX II-Remotekonsole verwaltet werden. Beachten Sie, dass Sie über die lokale Dominion KX II-Konsole auch Zugriff haben auf:

- Werksrücksetzung
- Lokale Porteinstellungen(auch für die Remotekonsole verfügbar)

Hinweis: Auf diese Funktionen können nur Benutzer mit Administratorrechten zugreifen.



Lokale Porteinstellungen der lokalen Dominion KX II-Konsole konfigurieren

Auf der Seite "Local Port Settings" (Lokale Porteinstellungen) können Sie viele Einstellungen für die lokale Dominion KX II-Konsole anpassen. Dazu zählen die Tastatur, die Zugriffstasten, die Verzögerung beim Videowechsel, der Stromsparmodus, die Auflösungseinstellungen für die lokale Benutzeroberfläche sowie die lokale Benutzerauthentifizierung.

Hinweis: Auf diese Funktionen können nur Benutzer mit Administratorrechten zugreifen.

So konfigurieren Sie die lokalen Porteinstellungen:

Hinweis: Einige Einstellungsänderungen, die auf der Seite "Local Port Settings" (Lokale Porteinstellungen) vorgenommen werden, führen zum Neustart des verwendeten Browsers. Führt eine Einstellungsänderung zum Neustart des Browser, so ist dies in den hier beschriebenen Schritten vermerkt.

1. Wählen Sie "Device Settings" > "Local Port Settings" (Geräteeinstellungen > Lokale Porteinstellungen) aus. Die Seite "Local Port Settings" (Lokale Porteinstellungen) wird angezeigt.
2. Wählen Sie aus den Optionen in der Dropdown-Liste den geeigneten Tastaturtyp aus. Der Browser wird neu gestartet, nachdem diese Änderung durchgeführt wurde.
   - US (USA)
   - US/International (USA/International)
   - United Kingdom (Großbritannien)
   - French (France) (Französisch)
   - German (Germany) (Deutsch, Deutschland)
   - JIS (Japanese Industry Standard) [Japanisch (Japanischer Branchenstandard)]
   - Simplified Chinese (Vereinfachtes Chinesisch)
   - Traditional Chinese (Traditionelles Chinesisch)
   - Dubeolsik Hangul (Korean) (Koreanisch)
   - German (Deutsch, Schweiz)
   - Portugiesisch (Portugal)
   - Norwegian (Norway) (Norwegisch)
   - Swedish (Sweden) (Schwedisch)
   - Danish (Denmark) (Dänisch)
   - Belgian (Belgium) (Belgisch)

Hinweis: Sie können die Tastatur für Chinesisch, Japanisch und Koreanisch nur für die Anzeige verwenden. Für Funktionen der lokalen Dominion KX II-Konsole werden Eingaben in diesen Sprachen derzeit nicht unterstützt.

3. Wählen Sie die Zugriffstaste für den lokalen Port. Über die Zugriffstaste für den lokalen Port können Sie zur Benutzeroberfläche der lokalen Dominion KX II-Konsole zurückkehren, wenn gerade eine Zielserveroberfläche angezeigt wird. Die Standardoption lautet "Double Click Scroll Lock" (Rollen-Taste zweimal drücken). Sie können jedoch eine andere Tastenkombination aus der Dropdownliste auswählen.

Zugriffstaste	Zu drückende Tastenkombination
Rollen-Taste zweimal drücken	Drücken Sie die Rollen-Taste zweimal kurz hintereinander.
Num-Feststelltaste zweimal drücken	Drücken Sie die Num-Feststelltaste zweimal kurz hintereinander.
Feststelltaste zweimal drücken	Drücken Sie die Feststelltaste zweimal kurz hintereinander.
Linke Alt-Taste zweimal drücken	Drücken Sie die linke Alt-Taste zweimal kurz hintereinander.
Linke Umschalttaste zweimal drücken	Drücken Sie die linke Umschalttaste zweimal kurz hintereinander.
Linke Strg-Taste zweimal drücken	Drücken Sie die linke Strg-Taste zweimal kurz hintereinander.

4. Wählen Sie die Verbindungstaste für den lokalen Port aus. Verwenden Sie eine Verbindungstastenfolge, um eine Verbindung mit einem Zielgerät herzustellen und zu einem anderen Zielgerät zu wechseln. Sie können anschließend die Zugriffstaste verwenden, um die Verbindung zum Zielgerät zu trennen und zur GUI des lokalen Ports zurückzukehren. Die Verbindungstaste ist für Standardserver und Blade-Chassis verfügbar. Wenn die Verbindungstaste für den lokalen Port erstellt wurde, erscheint diese im Navigationsfenster der GUI, sodass Sie sie als Referenz verwenden können. Beispiele für Verbindungstastenfolgen finden Sie unter ***Beispiele für Verbindungstasten*** (auf Seite 294).
5. Legen Sie ggf. im Feld "Video Switching Delay" (Verzögerung beim Videowechsel) einen Wert zwischen 0 und 5 Sekunden fest. Üblicherweise wird der Wert 0 verwendet, wenn nicht mehr Zeit benötigt wird (manche Monitore benötigen mehr Zeit, um das Videobild zu wechseln).
6. Führen Sie die folgenden Schritte aus, wenn Sie die Stromsparfunktion verwenden möchten:



a. Aktivieren Sie das Kontrollkästchen "Power Save Mode" (Stromsparmodus).

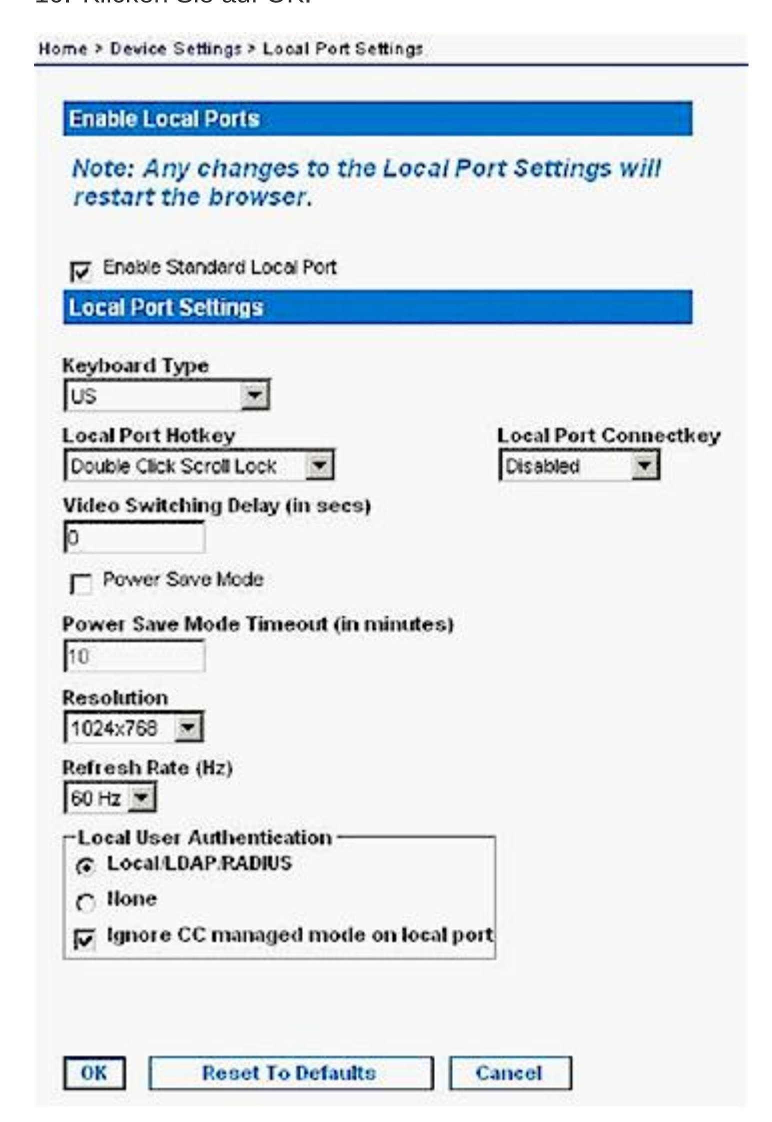
b. Legen Sie die Zeitspanne (in Minuten) fest, nach der in den Stromsparmodus geschaltet wird.

7. Wählen Sie in der Dropdown-Liste die Auflösung für die lokale Dominion KX II-Konsole aus: Der Browser wird neu gestartet, nachdem diese Änderung durchgeführt wurde.
   - 800 x 600
   - 1024 x 768
   - 1280 x 1024
8. Wählen Sie in der Dropdown-Liste die Aktualisierungsfrequenz aus. Der Browser wird neu gestartet, nachdem diese Änderung durchgeführt wurde.
   - 60 Hz
   - 75 Hz
9. Wählen Sie die Methode zur lokalen Benutzerauthentifizierung aus:
   - Local/LDAP/RADIUS (Lokal/LDAP/RADIUS): Dies ist die empfohlene Option. Weitere Informationen zur Authentifizierung finden Sie unter ***Remoteauthentifizierung*** (auf Seite 40).
   - Keine. Der lokale Konsolenzugriff wird nicht authentifiziert. Diese Option ist nur für sichere Umgebungen empfehlenswert.
   - Aktivieren Sie das Kontrollkästchen "Ignore CC managed mode on local port" (Modus zur Verwaltung über CC auf lokalem Port ignorieren), wenn Sie den lokalen Benutzerzugriff auf Dominion KX II ermöglichen möchten, auch wenn das Gerät über CC-SG verwaltet wird.

Hinweis: Wenn diese Option deaktiviert ist, Sie sie später jedoch aktivieren möchten, müssen Sie die CC-SG-Verwaltung für das Gerät beenden (von CC-SG aus). Anschließend können Sie das Kontrollkästchen aktivieren.



10. Klicken Sie auf OK.



Lokale Porteinstellungen von der lokalen Dominion KX II-Konsole konfigurieren

Der lokale Standardport und der erweiterte lokale Port können über die Remotekonsole auf der Seite "Port Configuration" (Portkonfiguration) oder über die lokale Konsole auf der Seite "Local Port Settings" (Lokale Porteinstellungen) konfiguriert werden. Weitere Informationen zur Konfigurierung dieser Ports finden Sie unter ***Lokale Porteinstellungen für Dominion KX II konfigurieren*** (auf Seite 225).



Werksrücksetzung der lokalen Dominion KX II-Konsole

Hinweis: Dieses Feature ist nur für die lokale Dominion KX II-Konsole verfügbar.

Dominion KX II bietet über die Benutzeroberfläche der lokalen Konsole verschiedene Rücksetzungsmodi.

Hinweis: Bevor Sie die Einheit auf die Werkseinstellungen zurücksetzen, sollten Sie das Prüfprotokoll speichern. Das Prüfprotokoll wird bei der Zurücksetzung auf die Werkseinstellungen gelöscht, und dieses Ereignis wird nicht protokolliert. Weitere Informationen zum Speichern des Prüfprotokolls finden Sie unter ***Prüfprotokoll****.*

So führen Sie eine Werksrücksetzung durch:

1. Wählen Sie "Maintenance" > "Factory Reset" (Wartung > Werksrücksetzung) aus. Die Seite "Factory Reset" (Werksrücksetzung) wird angezeigt.
2. Wählen Sie die entsprechende Rücksetzungsoption aus:

- Full Factory Reset (Vollständige Werksrücksetzung) – Damit entfernen Sie die gesamte Konfiguration und setzen das Gerät komplett auf die werkseitigen Standardeinstellungen zurück. Beachten Sie, dass Verwaltungsverbindungen mit CommandCenter dadurch unterbrochen werden. Da diese Rückstellung so umfassend ist, werden Sie dazu aufgefordert, den Vorgang zu bestätigen.
- Network Parameter Reset (Netzwerkparameterrücksetzung) – Damit setzen Sie die Netzwerkparameter des Geräts auf die Standardwerte zurück [Klicken Sie auf "Device Settings" > "Network Settings" (Geräteeinstellungen > Netzwerkeinstellungen), um auf diese Informationen zuzugreifen]:
  - IP Auto Configuration (Automatische IP-Konfiguration)
  - IP Address (IP-Adresse)
  - Subnet Mask (Subnetzmaske)
  - Gateway IP Address (Gateway-IP-Adresse)
  - Primary DNS Server IP Address (IP-Adresse des primären DNS-Servers)
  - Secondary DNS Server IP Address (IP-Adresse des sekundären DNS-Servers)
  - Discovery Port (Erkennungsport)
  - Bandwidth Limit (Maximale Bandbreite)
  - LAN Interface Speed & Duplex (LAN-Schnittstellengeschwindigkeit & Duplex)
  - Enable Automatic Failover (Automatisches Failover aktivieren)

- Ping Interval (Pingintervall, Sekunden)
- Timeout (Zeitlimit, Sekunden)

1. Klicken Sie auf "Reset" (Zurücksetzen), um fortzufahren. Da hierbei alle Netzwerkeinstellungen verloren gehen, werden Sie aufgefordert, die Werksrücksetzung zu bestätigen.
2. Klicken Sie zum Fortfahren auf OK. Nach Abschluss des Vorgangs wird das Dominion KX II-Gerät automatisch neu gestartet.

Zurücksetzen des Dominion KX II mithilfe der Taste "Reset" (Zurücksetzen)

Auf der Rückseite des Geräts befindet sich die Taste "Reset" (Zurücksetzen). Sie ist etwas zurückgesetzt, damit sie nicht unbeabsichtigt gedrückt wird (Sie benötigen einen spitzen Gegenstand, um die Taste zu betätigen).

Welche Maßnahmen ergriffen werden, wenn die Taste "Reset" (Zurücksetzen) gedrückt wird, legen Sie über die grafische Benutzeroberfläche fest. Siehe Encryption & Share (Verschlüsselung und Freigabe).

Hinweis: Bevor Sie die Einheit auf die Werkseinstellungen zurücksetzen, sollten Sie das Prüfprotokoll speichern. Das Prüfprotokoll wird bei der Zurücksetzung auf die Werkseinstellungen gelöscht, und dieses Ereignis wird nicht protokolliert. Weitere Informationen zum Speichern des Prüfprotokolls finden Sie unter Prüfprotokoll.

So setzen Sie das Gerät zurück:

1. Schalten Sie die Dominion KX II-Einheit aus.
2. Verwenden Sie einen spitzen Gegenstand, und halten Sie die Taste zum Zurücksetzen damit gedrückt.
3. Halten Sie die Taste zum Zurücksetzen gedrückt und schalten Sie gleichzeitig das Dominion KX II-Gerät wieder ein.



4. Halten Sie die Taste "Reset" (Zurücksetzen) weitere zehn Sekunden gedrückt. Wenn das Gerät zurückgesetzt wurde, ertönen zwei kurze Tonsignale.



Anhang A Technische Daten

In diesem Kapitel

Physische Spezifikationen

Dominion KX II-Spezifikationen

Teilenummer	Produktbeschreibung	UPC-Code	Stromversorgung	Gewicht	Produktabmessungen (B x T x H)	Liefergewicht	Lieferabmessungen (B x T x H)
DKX2-108	Dominion KX II mit 8 Ports, Netzwerk- und lokaler Portzugriff über einen Kanal; virtuelle Medien, zwei Netzteile	785813624109	Zwei Netzteile 100/240 V 50/60 Hz 0,6A 25 Watt	8,58 lbs	1,75 Zoll x 17,32 Zoll x 11,4 Zoll	14,3 lbs	22 Zoll x 16,6 Zoll x 6,5 Zoll
				3,9 kg	44mm x 439mm x 290mm	6,5 kg	559mm x 422mm x 165mm
DKX2-116	Dominion KX II mit 16 Ports, Netzwerk- und lokaler Portzugriff über einen Kanal; virtuelle	785813624055	Zwei Netzteile 100/240 V 50/60 Hz 0,6A 25,4 Watt	8,65 lbs	1,75 Zoll x 17,3 Zoll x 11,4 Zoll	14,85 lbs	22 Zoll x 16,6 Zoll x 6,5 Zoll
				3,9 kg	44mm x 439mm x	6,7 kg	559mm x 422mm x



Teilenummer	Produktbeschreibung	UPC-Code	Stromversorgung	Gewicht	Produktabmessungen (B x T x H)	Liefergewicht	Lieferabmessungen (B x T x H)
	Medien, zwei Netzteile				290mm		165mm
DKX2-132	Dominion KX II mit 32 Ports, Netzwerk- und lokaler Portzugriff über einen Kanal; virtuelle Medien, zwei Netzteile	785813624079	Zwei Netzteile 100/240 V 50/60 Hz 0,6A 26 Watt	9,0 lbs	1,75 Zoll x 17,3 Zoll x 11,4 Zoll	14,9 lbs	22 Zoll x 16,6 Zoll x 6,5 Zoll
				4,1 kg	44mm x 439mm x 290mm	6,8 kg	559mm x 422mm x 165mm
DKX2-216	Dominion KX II mit 16 Ports, Netzwerk- und lokaler Portzugriff über zwei Kanäle; virtuelle Medien, zwei Netzteile	785813624086	Zwei Netzteile 100/240 V 50/60 Hz 0,6A 26,3 Watt	8,65 lbs	1,75 Zoll x 17,3 Zoll x 11,4 Zoll	14,49 lbs	22 Zoll x 16,6 Zoll x 6,5 Zoll
				3,9 kg	44mm x 439mm x 290mm	6,6 kg	559mm x 422mm x 165mm
DKX2-232	Dominion KX II mit 32 Ports, Netzwerk- und lokaler Portzugriff über zwei Kanäle; virtuelle Medien, zwei Netzteile	785813625021	Zwei Netzteile 100/240 V 50/60 Hz (Optimal: 47–63 Hz) 0,6 A 27 Watt	9,0 lbs	1,75 Zoll x 17,3 Zoll x 11,4 Zoll	14,9 lbs	22 Zoll x 16,6 Zoll x 6,5 Zoll
				4,1 kg	44mm x 439mm x 290mm	6,8 kg	559mm x 422mm x 165mm
DKX2-416	Dominion KX II mit 16 Ports, Netzwerk- und lokaler Portzugriff über vier Kanäle; virtuelle Medien, zwei Netzteile	785813625359	Zwei Netzteile 100/240 V 50/60 Hz 1 A 62 Watt	9,04 lbs	17,3 Zoll x 11,6 Zoll x 1,75 Zoll	14,94 lbs	22 Zoll x 16,5 Zoll x 6,5 Zoll
				4,1 kg	440 mm x 295 mm x 44 mm	6,8 kg	560 mm x 420 mm x 165 mm

Teilenummer	Produktbeschreibung	UPC-Code	Stromversorgung	Gewicht	Produktabmessungen (B x T x H)	Liefergewicht	Lieferabmessungen (B x T x H)
DKX2-432	Dominion KX II mit 32 Ports, Netzwerk- und lokaler Portzugriff über vier Kanäle; virtuelle Medien, zwei Netzteile	785813625380	Zwei Netzteile 100/240 V 50/60 Hz 1 A 64 Watt	9,48 lbs	17,3 Zoll x 11,6 Zoll x 1,75 Zoll	15,38 lbs	22 Zoll x 16,5 Zoll x 6,5 Zoll
				4,3 kg	440 mm x 295 mm x 44 mm	7,0 kg	560 mm x 420 mm x 165 mm
DKX2-464	Dominion KX II mit 64 Ports, Netzwerk- und lokaler Portzugriff über vier Kanäle; virtuelle Medien, zwei Netzteile	785813625298	Zwei Netzteile 100/240 V 50/60 Hz 1 A 64 Watt	11,29 lbs	17,3 Zoll x 11,6 Zoll x 3,5 Zoll	19,8 lbs	22 Zoll x 16,5 Zoll x 6,5 Zoll
				5,12 kg	440 mm x 295 mm x 88 mm	9 kg	560 mm x 420 mm x 165 mm

KX2-8-Spezifikationen

Teilenummer	Produktbeschreibung	UPC-Code	Stromversorgung	Gewicht	Produktabmessungen (B x T x H)	Liefergewicht	Lieferabmessungen (B x T x H)
DKX2-832	Dominion KX II mit 32 Ports, Netzwerkzugriff über acht Kanäle; lokaler Standardport, erweiterter lokaler Port, virtuelle Medien, zwei Netzteile	0785813620019	Zwei Netzteile 100/240 V 50/60 Hz 1 A (0,5 A) 64 Watt	10,57 lbs	17,3 Zoll x 14,2 Zoll x 1,73 Zoll	35,90 lbs	22 Zoll x 18,5 Zoll x 11 Zoll
				4,8 kg	440 mm x 360 mm x 44 mm	16,3 kg	560 mm x 470 mm x 280 mm
DKX2-864	Dominion KX II mit 64 Ports, Netzwerkzugriff über acht Kanäle; lokaler Standardport, erweiterter	0785813620026	Zwei Netzteile 100/240 V 50/60 Hz 1,2 A 64 Watt	13,22 lbs	17,3 Zoll x 14,6 Zoll x 3,5 Zoll	22,47 lbs	21,7 Zoll x 20,1 Zoll x 7,5 Zoll
				6,0 kg	440 mm x 370 mm x 88 mm	10,2 kg	550 mm x 510 mm x 190 mm



Teilenummer	Produktbeschreibung	UPC-Code	Stromversorgung	Gewicht	Produktabmessungen (B x T x H)	Liefergewicht	Lieferabmessungen (B x T x H)
	lokaler Port, virtuelle Medien, zwei Netzteile						

Umgebungsanforderungen

Betrieb	
Temperatur	0° C bis 40° C
Luftfeuchtigkeit	20% bis 85% relative Luftfeuchtigkeit
Höhe über NN	Nicht zutreffend
Erschütterung	5-55-5 HZ, 0,38 mm, 1 Minute pro Zyklus; 30 Minuten für jede Achse (X, Y, Z)
Stoß	Nicht zutreffend
Lagerung	
Temperatur	0° C bis 50° C
Luftfeuchtigkeit	10 % bis 90 % relative Luftfeuchtigkeit
Höhe über NN	Nicht zutreffend
Erschütterung	5-55-5 HZ, 0,38 mm, 1 Minute pro Zyklus; 30 Minuten für jede Achse (X, Y, Z)
Stoß	Nicht zutreffend

Computer Interface Modules (CIMs)

Teilenummer	Produktbeschreibung	Produktgewicht	Produktabmessungen (B x T x H)	Liefergewicht	Lieferabmessungen (B x T x H)	UPC-Code
D2CIM-VUSB	Dominion KX II-CIM [USB-Port mit virtuellen Medien]	0,2 lbs	1,3 Zoll x 3,0 Zoll x 0,6 Zoll	0,2 lbs	7,2 Zoll x 9 Zoll x 0,6 Zoll	785813332004

Teilenummer	Produktbeschreibung	Produktgewicht	Produktabmessungen (B x T x H)	Liefergewicht	Lieferabmessungen (B x T x H)	UPC-Code
DCIM-PS2	Dominion KX I- & II-CIM [PS/2-Port]	0,2 lbs	1,3 Zoll x 3,0 Zoll x 0,6 Zoll	0,2 lbs	7,2 Zoll x 9 Zoll x 0,6 Zoll	785813338532
DCIM-USB	Dominion KX I- & II-CIM [USB-Port]	0,2 lbs	1,3 Zoll x 3,0 Zoll x 0,6 Zoll	0,2 lbs	7,2 Zoll x 9 Zoll x 0,6 Zoll	785813338518
DCIM-SUSB	Dominion KX I- & II-CIM [USB-Port für Sun]	0,2 lbs	1,3 Zoll x 3,0 Zoll x 0,6 Zoll	0,2 lbs	7,2 Zoll x 9 Zoll x 0,6 Zoll	785813338556
DCIM-USBG2	Dominion KX I- & II-CIM [USB-Port und USB-Port für Sun] G2-CIM	0,2 lbs	1,3 Zoll x 3,0 Zoll x 0,6 Zoll	0,2 lbs	7,2 Zoll x 9 Zoll x 0,6 Zoll	785813338884
DCIM-SUN	Dominion KX I- & II-CIM [Sun-Port, HD15-Video]	0,2 lbs	1,3 Zoll x 3,0 Zoll x 0,6 Zoll	0,2 lbs	7,2 Zoll x 9 Zoll x 0,6 Zoll	785813338549
D2CIM-PWR	Dominion KX II-CIM für Remote-Powerstrips	0,2 lbs	1,3 Zoll x 3,0 Zoll x 0,6 Zoll	0,2 lbs	7,2 Zoll x 9 Zoll x 0,6 Zoll	785813332011
D2CIM-VUSB-32PAC	Großpaket mit 32 D2CIM-VUSB	2,90 kg	(1,3 Zoll x 3,0 Zoll x 0,6 Zoll)*32	3,63 kg	21,65 Zoll x 12,20 Zoll x 4,33 Zoll	785813332028
D2CIM-VUSB-64PAC	Großpaket mit 64 D2CIM-VUSB	5,81 kg	(1,3 Zoll x 3,0 Zoll x 0,6 Zoll)*64	18,13 lb	22,64 Zoll x 9,45 Zoll x 12,99 Zoll	785813332035
D2CIM-DVUSB	Dominion KX II-CIM [Dual-USB-Port mit virtuellen Medien]	0,23 lbs, 105 g	3,53 Zoll x 1,68 Zoll x 0,76 Zoll 89,7 x 42,7 x 19,3 (mm)	0,25 lbs, 112,5 g	3,9 Zoll x 5,7 Zoll x 1,0 Zoll 100 x 145 x 27 (mm)	785813339508
D2CIM-DVUSB-32PAC	Großpaket mit 32 D2CIM-DVUSB	10,1 lbs, 4,6 kg	21,9 Zoll x 12,2 Zoll x 4,3 Zoll 555 x 310 x 110 (mm)	10,1 lbs, 4,6 kg	21,9 Zoll x 12,2 Zoll x 4,3 Zoll 555 x 310 x	785813332080



Teilenummer	Produktbeschreibung	Produktgewicht	Produktabmessungen (B x T x H)	Liefergewicht	Lieferabmessungen (B x T x H)	UPC-Code
					110 (mm)	
D2CIM-DVUSB -64PAC	Großpaket mit 64 D2CIM-DVUSB	22,5 lbs, 10,2 kg	9,4 Zoll x 22,6 Zoll x 13,0 Zoll 240 x 575 x 330 (mm)	22,5 lbs, 10,2 kg	9,4 Zoll x 22,6 Zoll x 13,0 Zoll 240 x 575 x 330 (mm)	785813332097

Unterstützte CIMs und Betriebssysteme (Zielserver)

Zusätzlich zu den neuen Dominion KX II-D2CIMs werden die meisten Paragon®- und Dominion KX I-CIMs unterstützt. Die folgende Tabelle enthält die unterstützten Betriebssysteme, CIMs, virtuellen Medien und Mausmodi auf Zielservern.

Hinweis: Bei Geräten der ersten Generation werden für Windows®- und Linux®-Zielserver nur 32-Bit-Betriebssysteme unterstützt.



Unterstützte Paragon-CIMs	Betriebssystem und serielle Geräte (wenn zutreffend)	Virtuelle Medien	Mausmodus "Absolut"	Mausmodus "Intelligent"	Mausmodus "Standard"
• P2CIM-PS2	• Windows XP® • Windows 2000® • Windows 2000 Server® • Windows 2003 Server® • Windows Vista® • Windows 7® • Windows 2008® • Red Hat® Enterprise Linux® 4 ES • Red Hat Enterprise Linux 5 • Open SUSE 10, 11 • Fedora® 8 - 11 • IBM® AIX™ • HP UX			✓	✓
• P2CIM-AUSB • UUSBPD	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 • Open SUSE 10, 11 • Fedora 8–11 • IBM AIX • HP UX • Mac® OS			✓	✓



Unterstützte Paragon-CIMs	Betriebssystem und serielle Geräte (wenn zutreffend)	Virtuelle Medien	Mausmodus "Absolut"	Mausmodus "Intelligent"	Mausmodus "Standard"
• UKVMPD (Version 0C4) *Hinweis: Version 0C5 funktioniert nicht mit Dominion KX II.*	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 • Open SUSE 10, 11 • Fedora 8–11			✓	✓
• P2CIM-SUN • P2CIM-SUSB	• Alle in Dominion KX I unterstützten Solaris™-Betriebssysteme				✓
• P2CIM-SER	• Serielle Geräte				



Unterstützte Dominion KX I-DCIMs	Zielserver	Virtuelle Medien	Mausmodus "Absolut"	Mausmodus "Intelligent"	Mausmodus "Standard"
• DCIM-PS2	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 • Open SUSE 10, 11 • Fedora Core 3 und höher • IBM AIX • HP UX			✓	✓
• DCIM-USB	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 • Open SUSE 10, 11 • Fedora 8–11 • Mac OS • IBM AIX • HP UX			✓	✓



Unterstützte Dominion KX I-DCIMs	Zielserver	Virtuelle Medien	Mausmodus "Absolut"	Mausmodus "Intelligent"	Mausmodus "Standard"
• DCIM-USBG2	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 • Open SUSE 10, 11 • Fedora 8–11 • Mac OS • Alle in Dominion KX I unterstützten Solaris-Betriebssysteme • IBM AIX • HP UX			✓	✓
Hinweis: DCIM-USBG2 und P2CIM-AUSB verfügen über einen kleinen Schiebeschalter auf der Rückseite des CIM. Stellen Sie den Switch bei PC-basierten USB-Zielservern auf P und bei Sun-USB-Zielservern auf S. Eine neue Switch-Position wird erst wirksam, wenn das CIM aus- und wieder eingeschaltet wird. Um das CIM aus- und wieder einzuschalten, entfernen Sie den USB-Stecker vom Zielserver und schließen Sie ihn nach einigen Sekunden erneut an.					
• DCIM-SUN • DCIM-SUSB	• Alle in Dominion KX I unterstützten Solaris-Betriebssysteme			✓	✓



Unterstützte Dominion KX II-D2CIMs	Zielserver und Remote-Powerstrips (wenn zutreffend)	Virtuelle Medien	Mausmodus "Absolut"	Mausmodus "Intelligent"	Mausmodus "Standard"
• D2CIM-VUSB	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Open SUSE 10, 11 • Fedora Core 3 und höher • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 • Mac OS	✓	✓ *	✓	✓
Hinweis: D2CIM-VUSB wird auf Sun™ (Solaris)-Zielservern nicht unterstützt. **Das Linux-Betriebssystem unterstützt nicht den Mausmodus "Absolute Mouse" (Absolut).*					
• D2CIM-DVUSB	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Open SUSE 10, 11 • Fedora 8–11 • Mac OS	✓	✓	✓	✓
• D2CIM-PWR	• Remote-Powerstrips				



Unterstützte Paragon-CIMS und Konfigurationen

Dominion KX II unterstützt die P2CIM-APS2DUAL- und P2CIM-AUSBDUAL-CIMs, die zwei RJ45-Verbindungen zu unterschiedlichen KVM-Switches enthalten. Die Unterstützung dieser CIMs beinhaltet einen zweiten Pfad für den Zugriff auf das Ziel, falls einer der KVM-Switches blockiert ist oder ein Fehler auftritt.

Paragon CIM	Unterstützung	Keine Unterstützung
P2CIM-APS2DUAL	• Server mit IBM®-PS/2-Tastatur- und -Mausports • Automatische Schräglaufkompensierung (wenn CIMs an Paragon II angeschlossen sind, nicht von einem Dominion KX II) • Mausmodus "Intelligent" • Mausmodus "Standard"	• Virtuelle Medien • Smart Cards • Mausmodus "Absolut" • Verwendung mit Blade-Chassis • Kaskadierte KVM-Konfigurationen
P2CIM-AUSBDUAL	• Server mit USB- oder SUN™-USB-Tastatur- und -Mausports • Automatische Schräglaufkompensierung (wenn CIMs an Paragon II angeschlossen sind, nicht von einem Dominion KX II) • Mausmodus "Intelligent" • Mausmodus "Standard"	• Virtuelle Medien • Smart Cards • Mausmodus "Absolut" • Verwendung mit Blade-Chassis • Kaskadierte KVM-Konfigurationen



Richtlinien für Dominion KX II zu Dominion KX II

Berücksichtigen Sie die folgenden Richtlinien zur Systemkonfiguration, wenn Sie Paragon-CIMs in einer Dominion KX II-zu-Dominion KX II-Konfiguration verwenden:

Gleichzeitiger Zugriff

Der gleichzeitige Zugriff gewährleistet, dass der gleichzeitige Zugriff auf Ziele für alle Ziele von allen Benutzergruppen untersagt ist.

- Beide Dominion KX II-KVM-Switches müssen gemäß derselben Richtlinie für gleichzeitigen Zugriff auf Ziele konfiguriert werden.
- Wenn der private Zugriff auf Ziele erforderlich ist, muss für beide KVM-Switches der PC-Freigabemodus auf "Private" (Privat) festgelegt werden. Siehe ***Encryption & Share (Verschlüsselung und Freigabe)*** (auf Seite 237).

Hinweis: Sie dürfen sich nicht auf die PC-Freigabeberechtigungen für Benutzergruppen verlassen, wenn der exklusive Zugriff mithilfe von P2CIM-APS2DUAL oder P2CIM-AUSBDUAL mit Dominion KX II gewährleistet werden muss.

Aktualisieren des CIM-Namens

Die P2CIM-APS2- und P2CIM-AUSB-Namen werden im CIM-Speicher abgelegt.   Es gibt zwei Speicherorte für die Paragon-Namenskonvention (12 Zeichen) und die Dominion KX II-Namenskonvention (32 Zeichen).

Bei der ersten Verbindung zu einem Dominion KX II wird der Paragon-Name aus dem Speicher aufgerufen und von Dominion KX II in den CIM-Speicherort geschrieben. Nachfolgende Abfragen des CIM-Namens oder Aktualisierungen des CIM-Namens vom Dominion KX II finden an dem von Dominion KX II verwendeten Speicherort statt. Dominion KX II führt am von Paragon II verwendeten Speicherort keine Aktualisierungen aus.

Wenn der CIM-Name von einem Dominion KX II aktualisiert wird, findet der andere Dominion KX II den aktualisierten Namen und ruft diesen ab, sobald die Verbindung zu diesem Ziel wieder hergestellt wird. Der Name wird erst zu diesem Zeitpunkt auf dem anderen Dominion KX II aktualisiert.

Portstatus und -verfügbarkeit

Der Portstatus, der auf der Dominion KX II-Seite "Port Access" (Portzugriff) entweder als "Up" (Ein) oder "Down" (Aus) angezeigt wird, wird aktualisiert, um anzuzeigen, ob das CIM eingeschaltet und mit dem Dominion KX II-Port verbunden ist.



Die Portverfügbarkeit, die auf der Dominion KX II-Seite "Port Access " (Portzugriff) als "Idle" (Inaktiv), "Busy" (Verwendet) oder "Connected" (Verbunden) angezeigt wird, wird nur aktualisiert, um die Aktivität auf dem Ziel anzuzeigen, das vom selben Dominion KX II initiiert wurde.

Wenn eine Verbindung zum Ziel vom anderen Dominion KX II vorhanden ist, wird die Verfügbarkeit geprüft, sobald ein Verbindungsversuch stattfindet. Der Zugriff wird gemäß der PC-Freigaberichtlinie des Dominion KX II verweigert oder zugelassen. Die Verfügbarkeit wird erst zu diesem Zeitpunkt auf dem anderen Dominion KX II aktualisiert.

Wenn der Zugriff verweigert wird, weil das Ziel verwendet wird, wird eine Benachrichtigung angezeigt.

Arbeiten mit CC-SG

Von CC-SG initiierte Vorgänge basieren auf dem Status, der Verfügbarkeit und dem CIM-Namen, die vom verwalteten Dominion KX II gemeldet werden. Wenn das Ziel mit zwei verwalteten Dominion KX II verbunden ist und die Geräte zu CC-SG hinzugefügt werden, werden zwei Knoten erstellt. Jeder Knoten enthält eine eigene zugeordnete oob-kvm-Schnittstelle. Sie können auch von jedem Dominion KX II einen einzelnen Knoten mit einer oob-kvm-Schnittstelle konfigurieren.

Wenn die Dominion KX II für den Modus "Private" (Privat) konfiguriert wurden, wird der Benutzer bei einem zweiten Verbindungsversuch benachrichtigt, dass die Verbindung nicht hergestellt werden kann und der Zugriff verweigert wurde.

Wenn mithilfe des Fensters "CC-SG Port Profile" (CC-SG-Portprofil) ein Portname geändert wird, wird der geänderte Name an das verwaltete Dominion KX II geleitet. Der entsprechende Portname des anderen Dominion KX II wird erst in CC-SG aktualisiert, wenn über die oob-kvm-Schnittstelle des anderen Dominion KX II ein Verbindungsversuch zum Zielport stattfindet.

Richtlinien für Dominion KX II zu Paragon II

P2CIM-APS2DUAL oder P2CIM-AUSBDUAL kann mit Dominion KX II und Paragon II verbunden werden.

Gleichzeitiger Zugriff

Sowohl Dominion KX II und Paragon II müssen gemäß derselben Richtlinie für gleichzeitigen Zugriff auf Ziele konfiguriert werden.

Betriebsmodus von Paragon II	Modusbeschreibung	Unterstützt?
Private (Privat)	Nur ein Benutzer kann jeweils auf einen Server oder ein anderes Gerät auf einem bestimmten Kanalport exklusiv	Unterstützt. Sowohl Paragon II und Dominion KX II müssen auf



Betriebsmodus von Paragon II	Modusbeschreibung	Unterstützt?
	zugreifen.	"Private" (Privat) festgelegt sein. Die Einstellung "Private" (Privat) wird für das Dominion KX II-Gerät, jedoch nicht für die Benutzergruppe übernommen. Paragon II verwendet die Farbe Rot, um den Status "Verwendet" oder die Farbe Grün, um den Status "Verfügbar" anzuzeigen.
PC-Share (PC-Freigabe)	Ein Server oder anderes Gerät auf einem bestimmten Kanalport kann von mehreren Benutzern ausgewählt und gesteuert werden, jedoch erhält jeweils nur ein Benutzer die Tastatur- und Maussteuerung.	Unterstützt. "PC Share Idle Timeout" (Zeitlimit für Inaktivität der PC-Freigabe), das auf Paragon II konfiguriert wird, wird nicht unterstützt. Beide Benutzer können die Tastatur- und Maussteuerung gleichzeitig verwenden. Paragon II verwendet die Farbe Grün, um den Status "Verfügbar" anzuzeigen. Dies wird auch angezeigt, wenn ein anderer Benutzer bereits auf das Ziel zugreift.
Public View (Öffentliche Ansicht)	Während ein Benutzer auf einen Server oder auf ein anderes Gerät auf einem bestimmten Kanalport zugreift, können andere Benutzer diesen Kanalport auswählen, und die Videoausgabe von diesem Gerät anzeigen. Jedoch kann nur der erste Benutzer die Tastatur- und	Nicht unterstützt. Dieser Modus kann nicht verwendet werden, wenn das CIM mit Paragon II und Dominion KX II verbunden ist. Paragon II verwendet die Farbe Gelb, um den



Betriebsmodus von Paragon II	Modusbeschreibung	Unterstützt?
	Maussteuerung verwenden, bis er die Verbindung trennt oder umschaltet.	P-Ansichtsmodus anzuzeigen.

Aktualisieren des CIM-Namens

- Von Paragon II aktualisierte CIM-Namen werden an dem CIM-Speicherort gespeichert und von dort abgerufen, der der Paragon-Namenskonvention entspricht.
- Von Dominion KX II aktualisierte CIM-Namen werden an dem CIM-Speicherort gespeichert und von dort abgerufen, der der >ProductName<-Namenskonvention entspricht.
- Aktualisierungen des CIM-Namens werden nicht zwischen Paragon II und Dominion KX II übertragen.

Unterstützte Betriebssysteme (Clients)

Die folgenden Betriebssysteme werden auf dem Virtual KVM Client und dem Multi-Platform-Client (MPC) unterstützt:

Client-Betriebssystem	Unterstützung virtueller Medien (VM) auf Client
Windows 7®	Ja
Windows XP®	Ja
Windows 2008®	Ja
Windows Vista®	Ja
Windows 2000 SP4® Server	Ja
Windows 2003® Server	Ja
Windows 2008® Server	Ja
Red Hat® Desktop 5.0	Ja. Lokales ISO-Abbild, Remote-Dateiserverinstallation direkt von Dominion KX II.
Red Hat Desktop 4.0	Ja. Lokales ISO-Abbild, Remote-Dateiserverinstallation direkt von Dominion KX II.
Open SUSE 10, 11	Ja. Lokales ISO-Abbild, Remote-Dateiserverinstallation direkt



Client-Betriebssystem	Unterstützung virtueller Medien (VM) auf Client
	von Dominion KX II.
Fedora® 8 - 11	Ja. Lokales ISO-Abbild, Remote-Dateiserverinstallation direkt von Dominion KX II.
Mac® OS	Nein
Solaris™	Nein

Das JRE™-Plug-in ist für Windows® 32-Bit- und 64-Bit-Betriebssysteme verfügbar. MPC und VKC können nur über einen 32-Bit-Browser und die 64-Bit-Browser IE7 oder IE8 gestartet werden.

Im Folgenden werden die Anforderungen von Java™ unter den Windows-Betriebssystemen (32 und 64 Bit) aufgelistet:

Modus	Betriebssystem	Browser
Windows x64 32-Bit-Modus	Windows XP®	• Internet Explorer® 6.0 SP1+ oder 7.0, IE 8 • Mozilla® 1.4.X oder 1.7+ • Netscape® 7.X • Firefox® 1.06 - 3
	Windows Server 2003®	• Internet Explorer 6.0 SP1++, IE 7, IE 8 • Mozilla 1.4.X oder 1.7+ • Netscape 7.X • Firefox 1.06 – 3
	Windows Vista®	• Internet Explorer 7.0 oder 8.0
	Windows 7®	• Internet Explorer 7.0 oder 8.0 • Firefox 1.06 – 3
Windows x64 64-Bit-Modus	Windows XP	64-Bit-Betriebssystem, 32-Bit-Browser: • Internet Explorer 6.0 SP1+, 7.0 oder 8.0 • Mozilla 1.4.X oder 1.7+ • Netscape 7.X • Firefox 1.06 – 3 64-Bit-Modus, 64-Bit-Browse
	Windows XP Professional®	
	Windows XP Tablet®	
	Windows Vista	
	Windows Server 2003	
	Windows Server 2008	



Modus	Betriebssystem	Browser
	Windows 7	r: • Internet Explorer 7.0 oder 8.0

Unterstützte Browser

Dominion KX II unterstützt die folgenden Browser:

- Internet Explorer® 6, 7 und 8
- Firefox® 1.5, 2.0 und 3.0 (bis Build 3.0.10)
- Mozilla® 1.7
- Safari® 2.0

Zertifizierte Modems

- USRobotics® 56K 5686E
- ZOOM® v90
- ZOOM v92
- USRobotics Sportster® 56K
- USRobotics Courier™ 56K

Vom erweiterten lokalen Port der Modelle KX2-832 und KX2-864 unterstützte Geräte

Der erweiterte lokale Port unterstützt die folgenden Geräte:

- KX2-832 und KX2-864.
- Paragon II User Station (P2-UST) – direkt an den erweiterten Port angeschlossen.
- Paragon II Enhanced User Station (P2-EUST) – direkt an den erweiterten Port angeschlossen.
- Cat5Reach URKVMG Receiver – direkt an den erweiterten Port angeschlossen.
- Paragon II analoger KVM-Switch (UMT) – Zielport an den erweiterten lokalen Port angeschlossen. Bietet die größte Reichweite für den Zugriff auf den erweiterten Port bei Verwendung mit der Paragon II Enhanced User Station.

Verbindungsentfernung zum Zielserver und Videoauflösung

Die maximal unterstützte Entfernung hängt von mehreren Faktoren ab. Dazu gehören der Typ/die Qualität des Kabels der Kategorie 5, der Servertyp und -hersteller, der Videotreiber und Monitor, die Umgebungsbedingungen und die Erwartungen des Benutzers. In der folgenden Tabelle wird die maximale Entfernung zum Zielserver für verschiedene Videoauflösungen und Aktualisierungsfrequenzen angegeben:

Videoauflösung	Aktualisierungsfrequenz	Maximale Entfernung
1600 x 1200	60	15 m
1280 x 1024	60	30 m
1024 x 768	60	45 m

Hinweis: Aufgrund der Vielzahl an Serverherstellern und -typen, Betriebssystemversionen, Videotreibern usw. sowie der subjektiven Auffassung von Videoqualität kann Raritan nicht für die Leistung bei allen Entfernungen in allen Umgebungen garantieren.

Von Dominion KX II unterstützte Videoauflösungen finden Sie unter ***Unterstützte Videoauflösungen*** (auf Seite 323).

Für den erweiterten lokalen Port der Geräte KX2-832 und KX2-864 empfohlene maximale Entfernungen

Erweitertes Gerät	1024 x 768 bei 60 Hz	1280 x 1024 bei 60 Hz
Paragon II UMT unter Verwendung einer EUST	1000	900
Paragon EUST	500	400
URKVM	650	250
Paragon UST	500	200

Remoteverbindung

Remoteverbindung	Details
Netzwerk	10BASE-T-, 100BASE-T- und 1000BASE-T



	(Gigabit)-Ethernet
Protokolle	TCP/IP, UDP, SNTP, HTTP, HTTPS, RADIUS, LDAP/LDAPS

Unterstützte Videoauflösungen

Stellen Sie sicher, dass die Videoauflösung und die Aktualisierungsfrequenz aller Zielserver von Dominion KX II unterstützt werden und das Signal keinen Zeilensprung beinhaltet.

Die Videoauflösung und die Kabellänge sind wichtige Faktoren für die Maussynchronisierung. Siehe ***Verbindungsentfernung zum Zielserver und Videoauflösung*** (auf Seite 322).

Die folgenden Auflösungen werden von Dominion KX II unterstützt:

Auflösungen	
640 x 350 bei 70Hz	1024 x 768 bei 75Hz
640 x 350 bei 85Hz	1024 x 768 bei 90Hz
640 x 400 bei 56Hz	1024 x 768 bei 100Hz
640 x 400 bei 84Hz	1152 x 864 bei 60Hz
640 x 400 bei 85Hz	1152 x 864 bei 70Hz
640 x 480 bei 60Hz	1152 x 864 bei 75Hz
640 x 480 bei 66,6Hz	1152 x 864 bei 85Hz
640 x 480 bei 72Hz	1152 x 870 bei 75,1Hz
640 x 480 bei 75Hz	1152 x 900 bei 66Hz
640 x 480 bei 85Hz	1152 x 900 bei 76Hz
720 x 400 bei 70Hz	1280 x 720 bei 60Hz
720 x 400 bei 84Hz	1280 x 960 bei 60Hz
720 x 400 bei 85Hz	1280 x 960 bei 85Hz

Auflösungen	
800 x 600 bei 56Hz	1280 x 1024 bei 60Hz
800 x 600 bei 60Hz	1280 x 1024 bei 75Hz
800 x 600 bei 70Hz	1280 x 1024 bei 85Hz
800 x 600 bei 72Hz	1360 x 768 bei 60Hz
800 x 600 bei 75Hz	1366 x 768 bei 60Hz
800 x 600 bei 85Hz	1368 x 768 bei 60Hz
800 x 600 bei 90Hz	1400 x 1050 bei 60Hz
800 x 600 bei 100Hz	1440 x 900 bei 60Hz
832 x 624 bei 75,1Hz	1600 x 1200 bei 60Hz
1024 x 768 bei 60Hz	1680 x 1050 bei 60Hz

Hinweis: Für Composite Sync- und Sync-on-Green-Video ist ein zusätzlicher Adapter erforderlich.

Hinweis: Einige Auflösungen stehen standardmäßig nicht zur Verfügung. Wird eine Auflösung nicht angezeigt, stecken Sie zuerst den Monitor an, stecken Sie den Monitor wieder aus und anschließend das CIM ein.

Hinweis: Werden die Auflösungen 1440 x 900 und 1680 x 1050 nicht angezeigt, jedoch von der Grafik-Adapterkarte des Zielservers unterstützt, ist möglicherweise ein DDC-1440- oder DDC-1680-Adapter erforderlich.



Unterstützte Tastatursprachen

Dominion KX II bietet Tastaturunterstützung für die in der folgenden Tabelle aufgeführten Sprachen.

Hinweis: Sie können die Tastatur für Chinesisch, Japanisch und Koreanisch nur für die Anzeige verwenden. Für Funktionen der lokalen Dominion KX II-Konsole werden Eingaben in diesen Sprachen derzeit nicht unterstützt. Weitere Informationen zu nicht US-amerikanischen Tastaturen finden Sie unter **Wichtige Hinweise** *(auf Seite 341).*

Hinweis: Raritan empfiehlt Ihnen für Änderungen der Spracheinstellungen die Verwendung von "system-config-keyboard", wenn Sie in einer Linux-Umgebung arbeiten.

Sprache	Regionen	Tastaturlayout
USA	Vereinigte Staaten von Amerika und die meisten englischsprachigen Länder: z. B. Kanada, Australien und Neuseeland.	US-amerikanisches Tastaturlayout
USA/International	Vereinigte Staaten von Amerika und die meisten englischsprachigen Länder: z. B. die Niederlande.	US-amerikanisches Tastaturlayout
Britisches Englisch	United Kingdom (Großbritannien)	Englisches Tastaturlayout (Großbritannien)
Traditionelles Chinesisch	Hongkong, Republik China (Taiwan)	Traditionelles Chinesisch
Vereinfachtes Chinesisch	Festland der Volksrepublik China	Vereinfachtes Chinesisch
Koreanisch	Südkorea	Dubeolsik Hangul
Japanisch	Japan	JIS-Tastatur (Japanischer Branchenstandard)
Französisch	Frankreich	Französisches (AZERTY-)Tastaturlayout
Deutsch (Deutschland)	Deutschland und Österreich	Deutsche Tastatur (QWERTZ-Layout)
Belgisch	Belgien	Belgisch
Norwegisch	Norwegen	Norwegisch

Sprache	Regionen	Tastaturlayout
Dänisch	Dänemark	Dänisch
Schwedisch	Schweden	Schwedisch
Ungarisch	Ungarn	Ungarisch
Slowenisch	Slowenien	Slowenisch
Italienisch	Italien	Italienisch
Spanisch	Spanien und die meisten spanischsprachigen Länder	Spanisch
Portugiesisch	Portugal	Portugiesisch

Smart Card-Lesegeräte

Unterstützte und nicht unterstützte Smart Card-Lesegeräte

KX II unterstützt nur externe Smart Card-USB-Lesegeräte.

Unterstützte Smart Card-Lesegeräte

Typ	Anbieter	Model (Modell)	Geprüft
USB	SCM Microsystems	SCR331	Geprüft für lokalen und Remotezugriff
USB	ActivIdentity®	ActivIdentity USB Reader v2.0	Geprüft für lokalen und Remotezugriff
USB	ActivIdentity	ActivIdentity USB Reader v3.0	Geprüft für lokalen und Remotezugriff
USB	Gemalto®	GemPC USB-SW	Geprüft für lokalen und Remotezugriff
USB-Tastatur mit Kartenlesegerät	Dell®	USB-Tastatur mit Smart Card-Lesegerät	Geprüft für lokalen und Remotezugriff
USB-Tastatur mit Kartenlesegerät	Cherry GmbH	G83-6744 SmartBoard	Geprüft für lokalen und Remotezugriff
USB-Lesegerät für Karten in SIM-Größe	Omnikey	6121	Geprüft für lokalen und Remotezugriff
Integriert (Dell Latitude D620)	O2Micro	OZ776	Nur Remotezugriff



Typ	Anbieter	Model (Modell)	Geprüft
USB	SCM Microsystems	SCR331	Geprüft für lokalen und Remotezugriff
PCMCIA	ActivIdentity	ActivIdentity PCMCIA Reader	Nur Remotezugriff
PCMCIA	SCM Microsystems	SCR243	Nur Remotezugriff

Hinweis: SCM Microsystems SCR331 Smart Card-Lesegeräte dürfen nur mit der SCM Microsystems-Firmware v5.25 verwendet werden.

Nicht unterstützte Smart Card-Lesegeräte

In dieser Tabelle finden Sie Lesegeräte, die von Raritan mit KX II getestet wurden, nicht funktioniert haben und deshalb nicht unterstützt werden. Wenn ein Smart Card-Lesegerät nicht in den Listen für unterstützte und nicht unterstützte Lesegeräte aufgeführt ist, bietet Raritan keine Gewähr für die Funktion des Lesegeräts mit KX II.

Typ	Anbieter	Model (Modell)	Hinweise
USB-Tastatur mit Kartenlesegerät	HP®	ED707A	Kein Interrupt-Endpunkt => nicht mit Microsoft®-Treiber kompatibel
USB-Tastatur mit Kartenlesegerät	SCM Microsystems	SCR338	Proprietäre Implementierung eines Kartenlesegeräts (nicht CCID-konform)
USB-Token	Aladdin®	eToken PRO™	Proprietäre Implementierung

Mindestanforderungen an das System

Anforderungen für den lokalen Port

Die grundlegende Kompatibilitätsanforderung für die Nutzung des lokalen Ports von Dominion KX II ist:

- Alle Geräte (Smart Card-Lesegeräte oder Token), die lokal angeschlossen werden, müssen USB CCID-konform sein.

Zielserver-Anforderungen

Die grundlegenden Kompatibilitätsanforderungen für die Verwendung von Smart Card-Lesegeräten am Zielserver sind:

- Der IFD-Handler (Smart Card-Lesegerät) muss ein standardmäßiger USB CCID-Gerätetreiber sein (vergleichbar mit dem Microsoft® USB CCID-Treiber).
- Ein D2CIM-DVUSB (Dual-VM CIM) ist erforderlich, das die Firmwareversion 3A6E oder höher verwendet.
- Wo ein CIM pro Blade verwendet wird, werden Blade-Chassis-Serververbindungen unterstützt.
- Blade-Chassis-Serververbindungen mit einem CIM pro Blade werden nur für die IBM® BladeCenter®-Modelle H und E mit aktivierter automatischer Erkennung unterstützt.

Windows XP-Ziele

Windows XP®-Betriebssystemziele müssen Windows XP SP3 ausführen, um Smart Cards mit Dominion KX II zu verwenden. Wenn Sie .NET 3.5 in einer Windows XP-Umgebung auf dem Zielserver verwenden, müssen Sie SP1 verwenden.

Linux-Ziele

Wenn Sie ein Linux®-Ziel verwenden, müssen die folgenden Voraussetzungen erfüllt sein, um Smart Card-Lesegeräte mit Dominion KX II zu verwenden.

- CCID-Anforderungen

  Wird das Raritan D2CIM-DVUSB VM/CCID von Ihrem Linux-Ziel nicht als Smart Card-Lesegerät erkannt, kann es erforderlich sein, den CCID-Treiber auf die Version 1.3.8 oder höher und die Treiberkonfigurationsdatei (Info.plist) zu aktualisieren.

Betriebssystem	CCID-Anforderungen
RHEL 5	CCID-1.3.8-1.el5
SuSE 11	PCSC-CCID-1.3.8-3.12
Fedora® Core 10	CCID-1.3.8-1.fc10.i386



Remoteclient-Anforderungen

Die grundlegenden Anforderungen für Kompatibilität am Remoteclient sind:

- Der IFD-Handler (Smart Card-Lesegerät) muss ein PC/SC-konformer Gerätetreiber sein.
- Die ICC-Ressourcenverwaltung (Smart Card) muss verfügbar und PC/SC-konform sein.
- Die JRE™ 1.6.x mit Smart Card API muss für die Verwendung durch die Raritan-Client-Anwendung verfügbar sein.

Linux-Clients

Wenn Sie einen Linux®-Client verwenden, müssen die folgenden Voraussetzungen erfüllt sein, um Smart Card-Lesegeräte mit Dominion KX II zu verwenden.

Hinweis: Die Benutzeranmeldung am Client beim Einführen der Karte kann möglicherweise länger dauern, wenn eine oder mehrere aktive KVM-Sitzungen mit Zielen bestehen. Dies ist darauf zurückzuführen, dass der Anmeldeprozess an diese Ziele ebenfalls bearbeitet wird.

- PC/SC-Anforderungen

Betriebssystem	Erforderliches PC/SC-System
RHEL 5	PCSC-Lite-1.4.4-0.1.el5
SuSE 11	PCSC-Lite-1.4.102-1.24
Fedora® Core 10	PCSC-Lite-1.4.102.3.fc10.i386

- Erstellen eines Links zu einer Java™-Bibliothek

  Nach der Aktualisierung von RHEL 4, RHEL 5 und FC 10 muss ein Soft-Link zur libpcsclite.so-Datei erstellt werden. Dieser könnte zum Beispiel folgendermaßen aussehen: ln –s /usr/lib/libpcsclite.so.1 /usr/lib/libpcsclite.so. Dabei wird davon ausgegangen, dass bei der Installation des Pakets die Bibliotheken in /usr/lib or /user/local/lib abgelegt werden.

- PC/SC-Daemon

  Nachdem der PCSC-Daemon (Ressourcenverwaltung in Framework) neu gestartet wurde, starten Sie Browser und MPC ebenfalls.

Verwendete TCP- und UDP-Ports



Port	Beschreibung
HTTP, Port 80	Dieser Port kann bei Bedarf konfiguriert werden. Siehe ***HTTP- und HTTPS-Porteinstellungen*** (auf Seite 165). Alle von Dominion KX II über HTTP (Port 80) empfangenen Anforderungen werden standardmäßig zur Gewährleistung der Sicherheit automatisch an HTTPS weitergeleitet. Dominion KX II beantwortet Anforderungen aus Gründen der Benutzerfreundlichkeit über Port 80. Auf diese Weise müssen Benutzer für den Zugriff auf Dominion KX II im URL-Feld keine Eingaben vornehmen. Die Sicherheit ist jedoch vollständig gewährleistet.
HTTPS, Port 443	Dieser Port kann bei Bedarf konfiguriert werden. Siehe ***HTTP- und HTTPS-Porteinstellungen*** (auf Seite 165). Dieser Port wird standardmäßig für verschiedene Zwecke verwendet, z. B. für den Webserver des HTML-Clients, das Herunterladen von Clientsoftware (MPC/VKC) auf den Clienthost oder die Übertragung von KVM- oder virtuellen Mediendatenströmen zum Client.
Dominion KX II-Protokoll (Raritan KVM-über-IP), konfigurierbarer Port 5000	Dieser Port wird zur Erkennung anderer Dominion-Geräte und zur Kommunikation zwischen Raritan-Geräten und -Systemen, einschließlich CC-SG, verwendet. Standardmäßig ist der Port 5000 eingestellt. Sie können jedoch jeden anderen TCP-Port konfigurieren, der nicht verwendet wird. Informationen zum Konfigurieren dieser Einstellung finden Sie unter Netzwerkeinstellungen.
SNTP (Zeitserver) über den konfigurierbaren UDP-Port 123	Dominion KX II bietet optional die Möglichkeit, die interne Uhr mit einem zentralen Zeitserver zu synchronisieren. Diese Funktion erfordert die Verwendung des UDP-Ports 123 (Standardport für SNTP), sie kann jedoch auch zur Verwendung eines anderen Ports Ihrer Wahl konfiguriert werden. **Optional**
LDAP/LDAPS über den konfigurierbaren Port 389 oder 936	Wenn Dominion KX II zur Remoteauthentifizierung von Benutzeranmeldungen über das LDAP-/LDAPS-Protokoll konfiguriert ist, wird Port 389 oder 636 verwendet. Das System kann jedoch auch zur Verwendung eines anderen Ports Ihrer Wahl konfiguriert werden. **Optional**
RADIUS über den konfigurierbaren Port 1812	Wenn Dominion KX II zur Remoteauthentifizierung von Benutzeranmeldungen über das RADIUS-Protokoll konfiguriert ist, wird Port 1812 verwendet. Das System kann jedoch auch zur Verwendung eines anderen Ports Ihrer Wahl konfiguriert werden. **Optional**
RADIUS-Kontoführung über den konfigurierbaren Port 1813	Wenn Dominion KX II zur Remoteauthentifizierung von Benutzeranmeldungen über das RADIUS-Protokoll konfiguriert ist und auch die RADIUS-Kontoführung zur Ereignisprotokollierung verwendet, wird Port 1813 oder ein zusätzlicher Port Ihrer Wahl zur Übertragung von Protokollbenachrichtigungen verwendet.
SYSLOG über den konfigurierbaren UDP-Port 514	Wenn Dominion KX II zum Senden von Meldungen an einen Syslog-Server konfiguriert ist, werden die angegebenen Ports für die Kommunikation verwendet (verwendet UDP-Port 514).



SNMP-Standard-UDP-Ports	Port 161 wird für eingehende/ausgehende SNMP-Lese- und -Schreibvorgänge, Port 162 für ausgehenden Datenverkehr für SNMP-Traps verwendet. **Optional**
TCP-Port 21	Port 21 wird für die Kommandozeilenschnittstelle des Dominion KX II verwendet (wenn Sie mit dem technischen Kundendienst von Raritan zusammenarbeiten).

Netzwerk-Geschwindigkeitseinstellungen

Netzwerk-Geschwindigkeitseinstellung von Dominion KX II							
Porteinstellung Netzwerkswitch		**Automatisch**	**1000/Voll**	**100/Voll**	**100/Halb**	**10/Voll**	**10/Halb**
	Automatisch	Höchste verfügbare Geschwindigkeit	1000/Voll	Dominion KX II: 100/Voll Switch: 100/Halb	100/Halb	Dominion KX II: 10/Voll Switch: 10/Halb	10/Halb
	1000/Voll	1000/Voll	1000/Voll	Keine Kommunikation	Keine Kommunikation	Keine Kommunikation	Keine Kommunikation
	100/Voll	Dominion KX II: 100/Halb Switch: 100/Voll	Dominion KX II: 100/Halb Switch: 100/Voll	100/Voll	Dominion KX II: 100/Halb Switch: 100/Voll	Keine Kommunikation	Keine Kommunikation
	100/Halb	100/Halb	100/Halb	Dominion KX II: 100/Voll Switch: 100/Halb	100/Halb	Keine Kommunikation	Keine Kommunikation
	10/Voll	Dominion KX II: 10/Halb Switch: 10/Voll	Keine Kommunikation	Keine Kommunikation	Keine Kommunikation	10/Voll	Dominion KX II: 10/Halb Switch: 10/Voll
	10/Halb	10/Halb	Keine Kommunikation	Keine Kommunikation	Keine Kommunikation	Dominion KX II: 10/Voll Switch: 10/Halb	10/Halb

Legende:

(weiß, dünner Rahmen)	Funktioniert nicht wie erwartet
(grün)	Unterstützt
(hellblau)	Funktionen; nicht empfohlen
(rot)	NICHT von Ethernet-Spezifikationen unterstützt; Produkt kommuniziert, es treten allerdings Kollisionen auf.
(weiß, dicker Rahmen)	Laut Ethernet-Spezifikation sollte hier "Keine Kommunikation" gelten, beachten Sie jedoch, dass das Verhalten des Dominion KX II vom erwarteten Verhalten abweicht.

Hinweis: Um eine zuverlässige Netzwerkkommunikation zu erhalten, konfigurieren Sie LAN-Schnittstellengeschwindigkeit und Duplex für Dominion KX II und den LAN-Switch auf den gleichen Wert. Konfigurieren Sie beispielsweise Dominion KX II und den LAN-Switch auf "Autodetect" (Automatische Erkennung, empfohlen) oder stellen Sie sie auf ein(e) feste(s) Geschwindigkeit/Duplex wie 100MB/s/Voll.



Anhang B Aktualisieren des LDAP-Schemas

Hinweis: Die in diesem Kapitel beschriebenen Verfahren sollten nur von erfahrenen Benutzern durchgeführt werden.

In diesem Kapitel

Zurückgeben von Benutzergruppeninformationen

Verwenden Sie die Informationen in diesem Abschnitt, um Benutzergruppeninformationen zurückzugeben (und die Autorisierung zu unterstützen), sobald die Authentifizierung erfolgreich war.

Von LDAP

Wenn eine LDAP/LDAPS-Authentifizierung erfolgreich ist, bestimmt Dominion KX II die Berechtigungen eines Benutzers anhand der Berechtigungen der Gruppe des Benutzers. Ihr Remote-LDAP-Server kann diese Benutzergruppennamen bereitstellen, indem er ein wie folgt benanntes Attribut zurückgibt:

rciusergroup attribute type: string

Dies erfordert ggf. eine Schemaerweiterung auf Ihrem LDAP/LDAPS-Server. Bitten Sie den Administrator des Authentifizierungsservers, dieses Attribut zu aktivieren.

Von Microsoft Active Directory

Hinweis: Diese Aktualisierung sollte nur von einem erfahrenen Active Directory®-Administrator durchgeführt werden.

Die Rückgabe von Benutzergruppeninformationen von Microsoft® Active Directory für Windows 2000®-Server erfordert die Aktualisierung des LDAP-/LDAPS-Schemas. Weitere Informationen finden Sie in Ihrer Microsoft-Dokumentation.

1. Installieren Sie das Schema-Plug-in für Active Directory. Entsprechende Anweisungen finden Sie in der Dokumentation für Microsoft Active Directory.



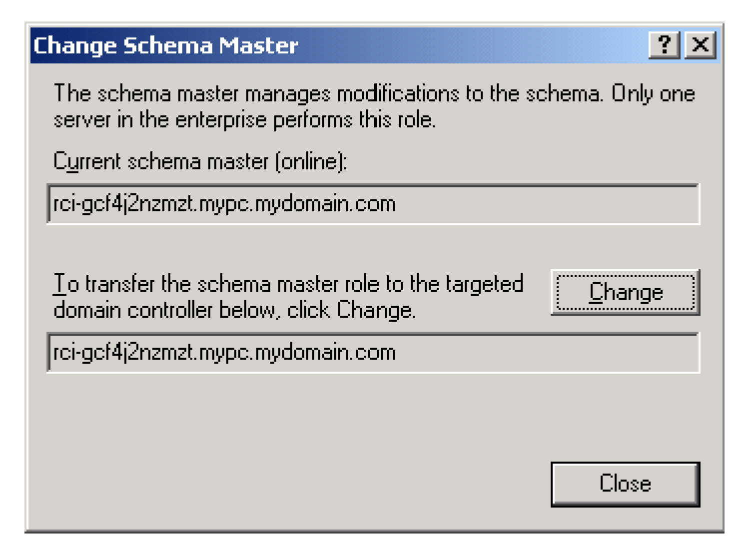
2. Starten Sie Active Directory Console und wählen Sie "Active Directory Schema" (Active Directory-Schema) aus.

Einstellen der Registrierung, um Schreibvorgänge im Schema zuzulassen

Um einem Domänencontroller das Schreiben im Schema zu erlauben, müssen Sie einen Registrierungseintrag erstellen, der Schemaaktualisierungen zulässt.

So lassen Sie Schreibvorgänge im Schema zu:

1. Klicken Sie mit der rechten Maustaste auf den Stammknoten des Active Directory® Schema im linken Fensterbereich, und wählen Sie "Operations Master" (Betriebsmaster) aus dem Kontextmenü aus. Das Dialogfeld "Change Schema Master" (Schemamaster ändern) wird angezeigt.



2. Aktivieren Sie das Kontrollkästchen "Schema can be modified on this Domain Controller" (Schema kann auf diesem Domänencontroller geändert werden). **Optional**
3. Klicken Sie auf OK.

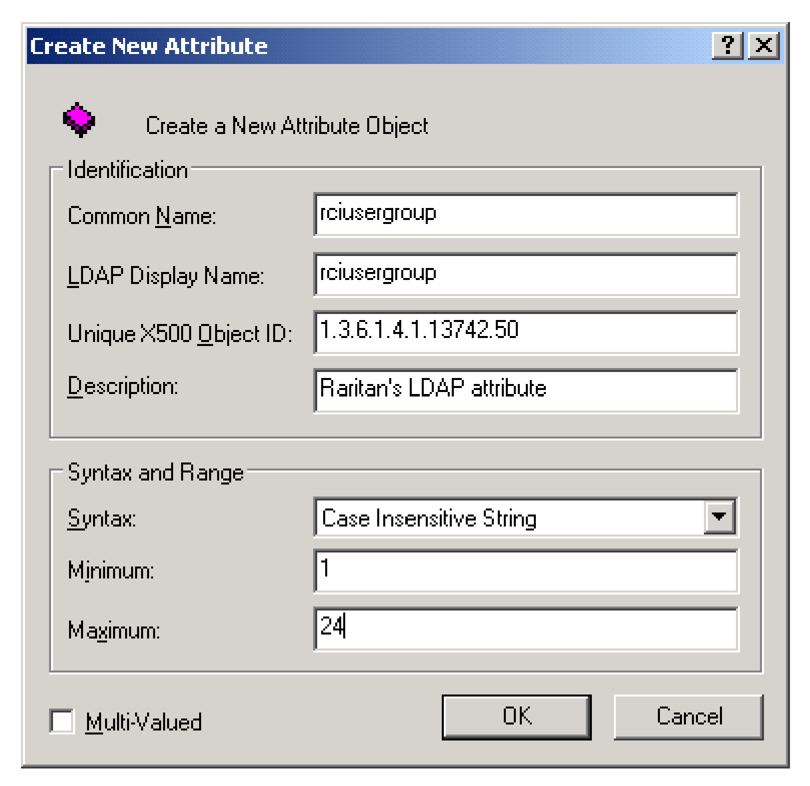
Erstellen eines neuen Attributs

So erstellen Sie neue Attribute für die Klasse "rciusergroup":

1. Klicken Sie im linken Fensterabschnitt auf das +-Symbol vor Active Directory® Schema.
2. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf "Attributes" (Attribute).



3. Klicken Sie auf "New" (Neu) und wählen Sie "Attribute" (Attribut) aus. Klicken Sie im angezeigten Hinweisfenster auf "Continue" (Weiter). Das Dialogfeld "Create New Attribute" (Neues Attribut erstellen) wird geöffnet.

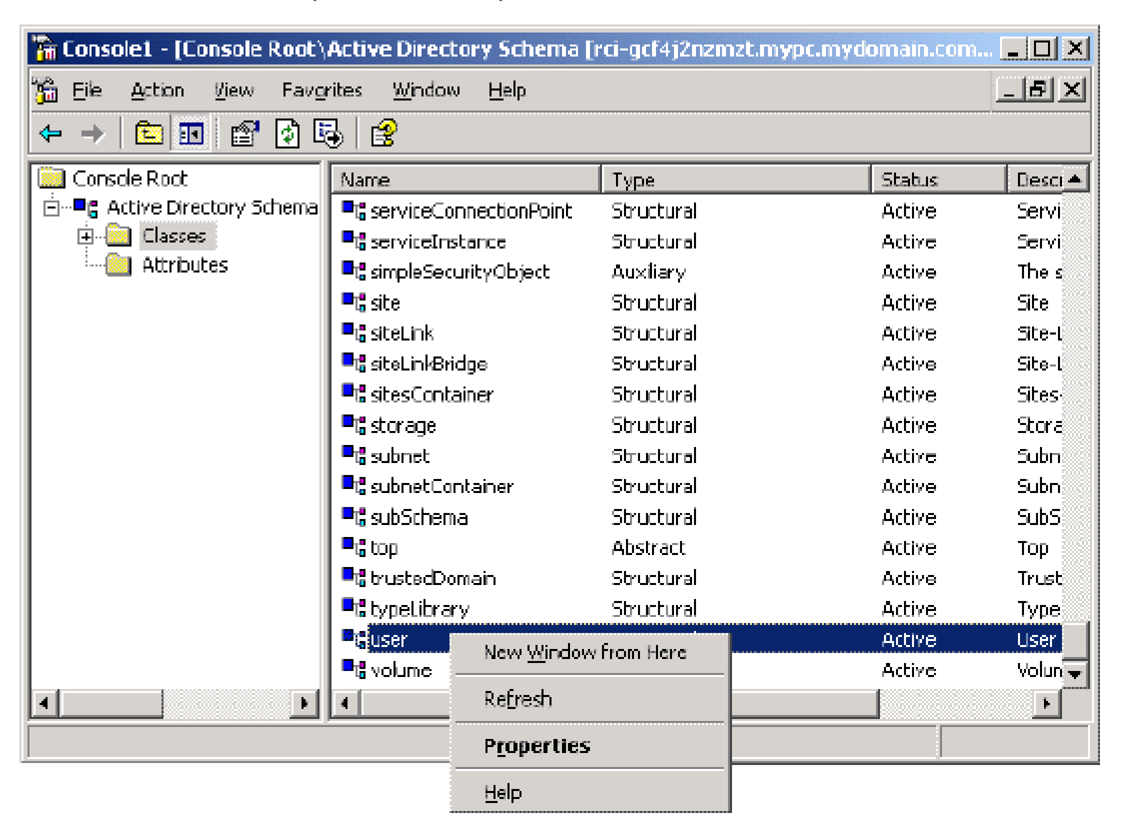


4. Geben Sie im Feld "Common Name" (Allgemeiner Name) den Wert *rciusergroup* ein.
5. Geben Sie im Feld "LDAP Display Name" (LDAP-Anzeigename) den Wert *rciusergroup* ein.
6. Geben Sie im Feld "Unique x5000 Object ID" (Eindeutige X500-OID) den Wert *1.3.6.1.4.1.13742.50* ein.
7. Geben Sie eine aussagekräftige Beschreibung im Feld "Description" (Beschreibung) ein.
8. Klicken Sie auf die Dropdownliste "Syntax" und wählen Sie "Case Insensitive String" (Groß-/Kleinschreibung nicht beachten) aus.
9. Geben Sie im Feld "Minimum" den Wert *1* ein.
10. Geben Sie im Feld "Maximum" den Wert *24* ein.
11. Klicken Sie zum Erstellen des neuen Attributs auf OK.

Hinzufügen von Attributen zur Klasse

So fügen Sie der Klasse Attribute hinzu:

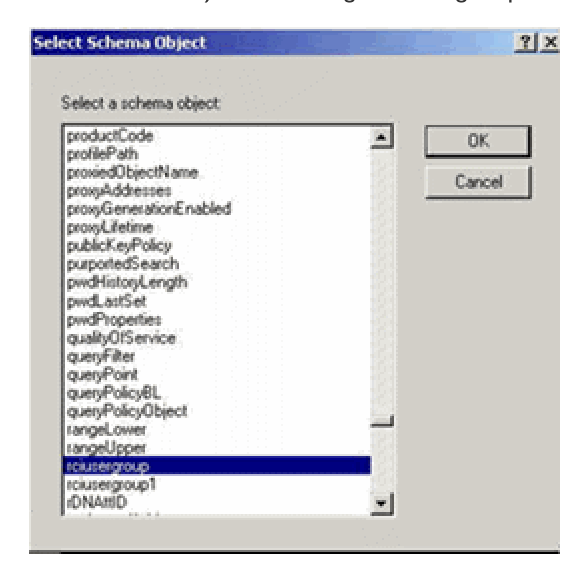
1. Klicken Sie im linken Fensterbereich auf "Classes" (Klassen).
2. Suchen Sie im rechten Fensterbereich den Wert "User Class" (Benutzerklasse) und klicken Sie mit der rechten Maustaste darauf.



3. Wählen Sie "Properties" (Eigenschaften) aus dem Kontextmenü. Das Dialogfeld "User Properties" (Benutzereigenschaften) wird geöffnet.
4. Klicken Sie auf die Registerkarte "Attributes" (Attribute), um diese zu öffnen.
5. Klicken Sie auf "Add" (Hinzufügen).



6. Wählen Sie in der Liste "Select Schema Object" (Schemaobjekt auswählen) den Eintrag "rciusergroup" aus.



7. Klicken Sie im Dialogfeld "Select Schema Object" (Schemaobjekt auswählen) auf OK.
8. Klicken Sie im Dialogfeld "User Properties" (Benutzereigenschaften) auf OK.

Aktualisieren des Schemacache

▶ So aktualisieren Sie den Schemacache:

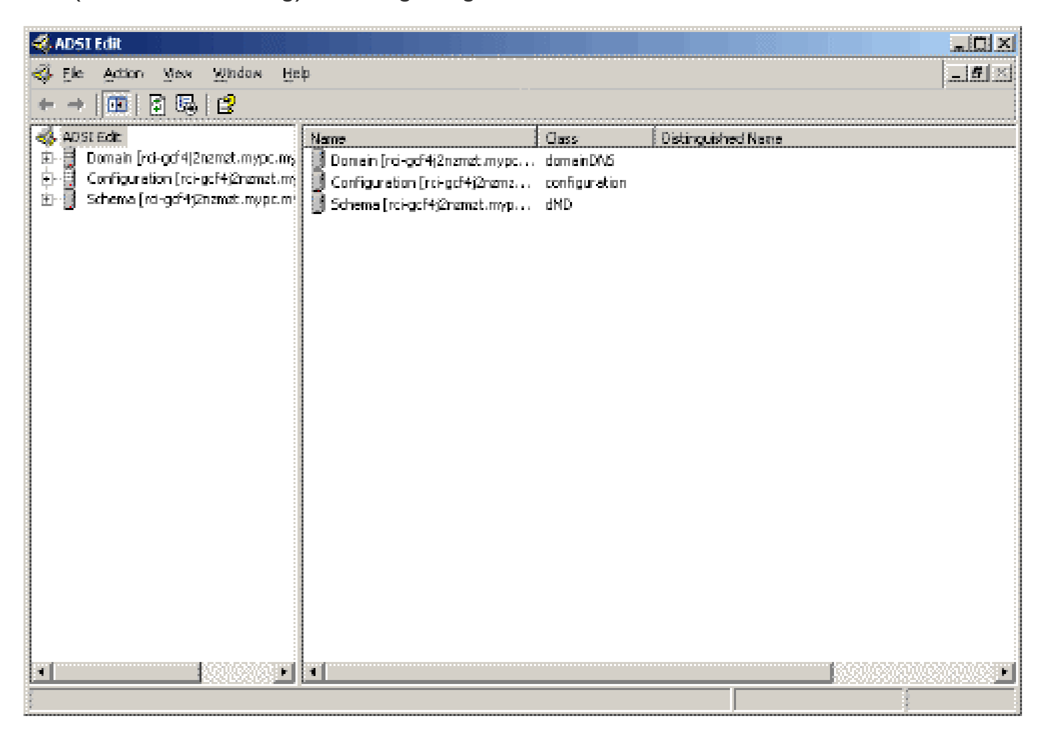
1. Klicken Sie im linken Fensterbereich mit der rechten Maustaste auf "Active Directory® Schema", und wählen Sie "Reload the Schema" (Schema neu laden) aus.
2. Minimieren Sie die Active Directory-Schema-MMC-Konsole (Microsoft® Management Console).

Bearbeiten von rciusergroup-Attributen für Benutzermitglieder

Verwenden Sie zum Ausführen des Active Directory®-Skripts auf einem Windows 2003®-Server das von Microsoft® bereitgestellte Skript (verfügbar auf der Windows 2003-Serverinstallations-CD). Diese Skripts werden bei der Installation von Microsoft Windows 2003 mit installiert. ADSI (Active Directory Service Interface) fungiert hierbei als Low-Level-Editor für Active Directory und ermöglicht so das Durchführen allgemeiner Verwaltungsaufgaben wie Hinzufügen, Löschen und Verschieben von Objekten mit einem Verzeichnisdienst.

So bearbeiten Sie die einzelnen Benutzerattribute innerhalb der Gruppe "rciusergroup":

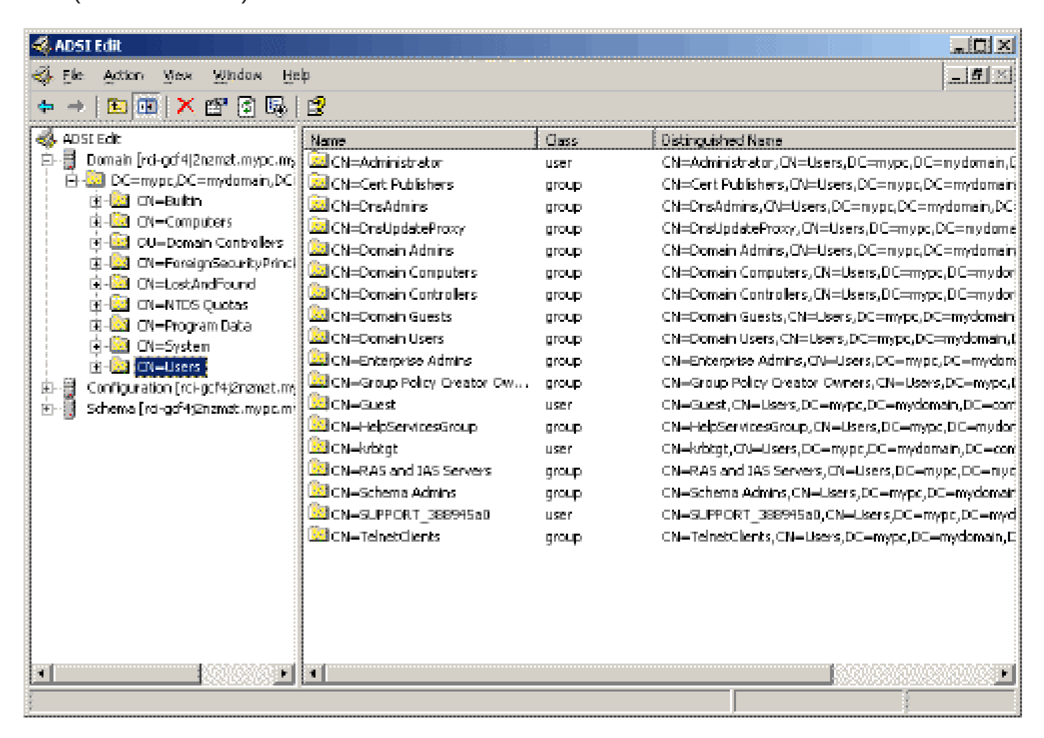
1. Wählen Sie auf der Installations-CD "Support" > "Tools" aus.
2. Doppelklicken Sie zur Installation der Support-Tools auf "SUPTOOLS.MSI".
3. Wechseln Sie zum Installationsverzeichnis der Support-Tools. Führen Sie "adsiedit.msc" aus. Das Fenster "ADSI Edit" (ADSI-Bearbeitung) wird angezeigt.



4. Öffnen Sie die Domäne.

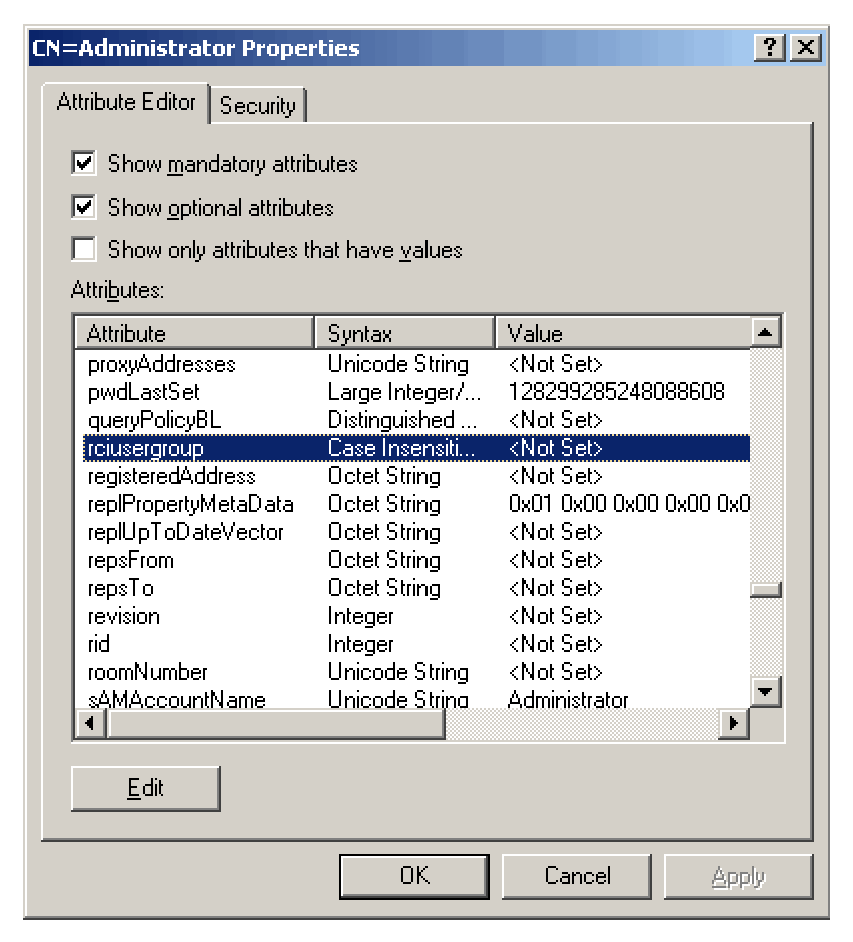


5. Klicken Sie im linken Fensterbereich auf den Ordner "CN=Users" (CN=Benutzer).



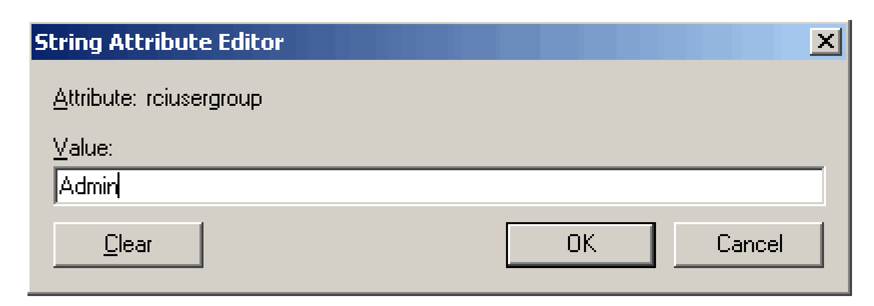
6. Navigieren Sie im rechten Fensterbereich zu dem Namen des Benutzers, dessen Eigenschaften geändert werden sollen. Klicken Sie mit der rechten Maustaste auf den Benutzernamen, und wählen Sie "Properties" (Eigenschaften) aus dem Kontextmenü aus.

7. Klicken Sie auf die Registerkarte "Attribute Editor" (Attributeditor), um sie anzuzeigen, wenn sie noch nicht geöffnet ist. Wählen Sie in der Liste "Attributes" (Attribute) "rciusergroup" aus.



8. Klicken Sie auf "Edit" (Bearbeiten). Das Dialogfeld "String Attribute Editor" (Attributeditor für Zeichenfolgen) wird angezeigt.

9. Geben Sie die Benutzergruppe (erstellt in Dominion KX II) in das Feld "Edit Attribute" (Attribut bearbeiten) ein. Klicken Sie auf OK.





Anhang C Wichtige Hinweise

In diesem Kapitel

Überblick

Dieser Abschnitt enthält wichtige Hinweise zur Verwendung des Dominion KX II. Zukünftige Aktualisierungen werden dokumentiert und sind online über den Link "Help" (Hilfe) auf der Benutzeroberfläche der Dominion KX II-Remotekonsole verfügbar.

Java Runtime Environment (JRE)

Wichtig: Sie sollten die Zwischenspeicherung für Java™ deaktivieren und den Java-Cache leeren. Weitere Informationen finden Sie in der Java-Dokumentation oder im Benutzerhandbuch "KVM and Serial Access Clients Guide".

Für die Dominion KX II-Remotekonsole und den MPC ist die Java Runtime Environment™ (JRE) erforderlich. Die Java-Version wird von der Dominion KX II-Remotekonsole überprüft. Falls die Version falsch oder veraltet ist, werden Sie dazu aufgefordert, eine kompatible Version herunterzuladen.

Raritan empfiehlt zur Gewährleistung einer optimalen Leistung die Verwendung von JRE Version 1.6, die Dominion KX II-Remotekonsole und der MPC funktionieren jedoch auch mit JRE Version 1.6.x oder höher (mit Ausnahme von 1.6.2).

Hinweis: Damit mehrsprachige Tastaturen in der Dominion KX II-Remotekonsole (Virtual KVM Client) funktionieren, müssen Sie die mehrsprachige Version von JRE installieren.

Hinweise zur Unterstützung von IPv6

Java

Java™ 1.6 unterstützt IPv6 bei folgenden Produkten:

- Solaris™ 8 oder höher
- Linux® Kernel 2.1.2 und höher (RedHat 6.1 und höher)

Java 5.0 und höher unterstützen IPv6 bei folgenden Produkten:

- Solaris 8 oder höher
- Linux Kernel 2.1.2 und höher (Kernel 2.4.0 und höher wird für bessere IPv6-Unterstützung empfohlen.)
- Betriebssysteme Windows XP® SP1 und Windows 2003®, Windows Vista®

Die folgenden IPv6-Konfigurationen werden *nicht* von Java unterstützt:

- J2SE 1.4 unterstützt kein IPv6 auf Microsoft® Windows®.

Linux

- Es wird empfohlen, bei Nutzung von IPv6 Linux Kernel 2.4.0 oder höher zu verwenden.
- Ein IPv6-aktivierter Kernel muss installiert werden, oder der Kernel muss mit aktivierten IPv6-Optionen wiederhergestellt werden.
- Bei der Verwendung von IPv6 und Linux müssen außerdem einige Netzwerkdienste installiert werden. Weitere Informationen finden Sie unter http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/IPv6-HOWTO.html.

Windows

- Windows XP- und Windows 2003-Benutzer müssen Microsoft Service Pack für IPv6 installieren, um IPv6 zu aktivieren.

Mac Leopard

- Die Dominion KX II-Version 2.0.20 unterstützt für Mac® Leopard® kein IPv6.

Samba

- Bei der Verwendung von Samba zusammen mit virtuellen Medien wird kein IPv6 unterstützt.



Tastaturen

Tastaturen (nicht USA)

Französische Tastatur

Zirkumflexzeichen (nur Linux®-Clients)

Virtual KVM Client und Multi-Platform-Client (MPC) unterstützen bei Verwendung einer französischen Tastatur mit Linux-Clients nicht die Tastenkombination "Alt Gr+9" für das Zirkumflexzeichen (^).

► **So stellen Sie das Zirkumflexzeichen dar:**

Drücken Sie auf einer französischen Tastatur die ^-Taste (rechts neben der P-Taste) und unmittelbar danach die Leertaste.

Alternativ können Sie ein Makro erstellen, das aus folgender Befehlsabfolge besteht:

1. Rechte Alt-Taste drücken
2. Taste "9" drücken
3. Taste "9" loslassen
4. Rechte Alt-Taste loslassen

Hinweis: Dieser Vorgang kann bei der Verwendung des Zirkumflexzeichens mit anderen Buchstaben (als Akzent über Vokalen) nicht durchgeführt werden. In diesem Fall verwenden Sie die ^-Taste (rechts neben der P-Taste) auf französischen Tastaturen.

Akzentzeichen (nur Windows XP®-Betriebssystem-Clients)

Im Virtual KVM Client und Multi-Platform-Client wird bei Verwendung der Tastenkombination "Alt Gr+7" das Akzentzeichen zweimal dargestellt, wenn eine französische Tastatur für Windows XP-Clients verwendet wird.

Hinweis: Dies trifft nicht auf Linus-Clients zu.

Nummernblock

Im Virtual KVM Client und Multi-Platform-Client werden die Zeichen auf dem Nummernblock bei französischen Tastaturen wie folgt dargestellt:

Zeichen auf dem Nummernblock	Dargestellt als
/	;

.	;

Tilde

Im Virtual KVM Client und Multi-Platform-Client wird bei Verwendung einer französischen Tastatur durch die Tastenkombination "Alt Gr+2" nicht die Tilde (~) angezeigt.

▶ So stellen Sie die Tilde dar:

Erstellen Sie mit der folgenden Befehlsabfolge ein Makro:

- Rechte Alt-Taste drücken
- Taste "2" drücken
- Taste "2" loslassen
- Rechte Alt-Taste loslassen

Einstellungen der Tastatursprache (Fedora Linux-Clients)

Da mit der Sun™-JRE™ auf einem Linux®-Betriebssystem Probleme bei der korrekten Erzeugung von KeyEvents (Tastenereignissen) für fremdsprachige Tastaturen auftreten, die mithilfe der Systemeinstellungen konfiguriert wurden, empfiehlt Raritan die Konfiguration fremdsprachiger Tastaturen mithilfe der in der folgenden Tabelle beschriebenen Methoden.

Sprache	Konfigurationsmethode
USA/Int.	Standard
Britisches Englisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Französisch	Keyboard Indicator (Tastaturanzeige)
Deutsch (Deutschland)	Keyboard Indicator (Tastaturanzeige)
Ungarisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Spanisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Deutsch (Schweiz)	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Norwegisch	Keyboard Indicator (Tastaturanzeige)
Schwedisch	Keyboard Indicator (Tastaturanzeige)
Dänisch	Keyboard Indicator (Tastaturanzeige)
Japanisch	System Settings (Control Center)



Sprache	Konfigurationsmethode
USA/Int.	Standard
	[Systemeinstellungen (Steuerzentrale)]
Koreanisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Slowenisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Italienisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]
Portugiesisch	System Settings (Control Center) [Systemeinstellungen (Steuerzentrale)]

Hinweis: Die Tastaturanzeige sollte bei Linux-Systemen, die Gnome als Desktopumgebung nutzen, verwendet werden.

Bei Verwendung einer ungarischen Tastatur mit einem Linux-Client werden die lateinischen Buchstaben "U" mit Doppelakut und "O" mit Doppelakut nur dargestellt, wenn JRE 1.6 verwendet wird.

Es gibt mehrere Methoden, die Einstellungen der Tastatursprache bei Fedora® Linux-Clients festzulegen. Die folgende Methode muss angewendet werden, um die Tasten für den Virtual KVM Client und den Multi-Platform Client (MPC) korrekt zuzuordnen.

So legen Sie die Tastatursprache unter "System Settings" (Systemeinstellungen) fest:

1. Wählen Sie in der Symbolleiste "System" > "Preferences" > "Keyboard" (System > Einstellungen > Tastatur) aus.
2. Öffnen Sie die Registerkarte "Layouts" (Tastatursprache).
3. Wählen Sie die entsprechende Sprache aus oder fügen Sie sie hinzu.
4. Klicken Sie auf "Close" (Schließen).

So legen Sie die Tastatursprache unter "Keyboard Indicator" (Tastaturanzeige) fest:

1. Klicken Sie mit der rechten Maustaste auf die Taskleiste und wählen Sie "Add to Panel" (Zu Panel hinzufügen) aus.
2. Klicken Sie im Dialogfeld "Add to Panel" (Zu Panel hinzufügen) mit der rechten Maustaste auf "Keyboard Indicator" (Tastaturanzeige) und wählen Sie aus dem Kontextmenü "Open Keyboard Preferences" (Tastatureinstellungen öffnen) aus.
3. Klicken Sie im Dialogfeld "Keyboard Preferences" (Tastatureinstellungen) auf die Registerkarte "Layouts" (Tastatursprache).

4. Fügen Sie Sprachen wie gewünscht hinzu oder löschen Sie sie.

Macintosh-Tastatur

Wenn Macintosh® als Client verwendet wird, funktionieren die folgenden Tasten auf der Mac®-Tastatur unter Verwendung von Java™ Runtime Environment (JRE™) nicht.

- F9
- F10
- F11
- F14
- F15
- Volume Up (Lautstärke höher)
- Volume Down (Lautstärke niedriger)
- Mute (Stummschaltung)
- Eject (Ausgabe)

Deshalb können diese Tasten bei Verwendung von Virtual KVM Client und Multi-Platform Client (MPC) zusammen mit einer Mac-Clienttastatur nicht verwendet werden.

Mauszeigersynchronisierung (Fedora)

Wenn bei Verwendung von Fedora® 7 eine Verbindung zu einem Zielserver über den Zwei-Cursor-Modus besteht, kann die Synchronisierung der lokalen und Ziel-Cursor nach einiger Zeit unterbrochen werden.

So synchronisieren Sie die Cursor erneut:

- Verwenden Sie die Option "Synchronize Mouse" (Maus synchronisieren) im Virtual KVM Client.

In der folgenden Tabelle werden die Mausmodi des Dominion KX II zusammengefasst und es wird angegeben, ob die Synchronisierung bei den jeweiligen Modi erhalten bleibt, wenn unter Verwendung von Fedora auf KVM-Zielserver zugegriffen wird.

Mausmodus	Fedora Core 5	Fedora Core 6
Absolute Mouse Synchronization (Absolute Maussynchronisierung)	Nein	Nein
Mausmodus "Intelligent"	Nein	Ja
Mausmodus "Standard"	Ja	Nein



Kabellängen und Videoauflösungen für Dell-Chassis

Um gute Videoqualität zu erreichen, empfiehlt Raritan die Verwendung der folgenden Kabellängen und Videoauflösungen, wenn Sie von Dominion KX II eine Verbindung mit Dell®-Blade-Chassis herstellen:

Kabellänge	Videoauflösung
1524,00 cm (9,1 m)	1024 x 768 x 60
1524,00 cm (9,1 m)	1280 x 1024 x 60
30 ft (9,1 m)	1600 x 1200 x 60

Fedora

Beheben von Fokusproblemen bei Fedora Core

Bei Verwendung des Multi-Platform-Client (MPC) kann es vorkommen, dass Sie sich nicht am Dominion KX II-Gerät anmelden oder auf KVM-Zielserver zugreifen können (Windows®, SUSE usw.). Außerdem wird durch Drücken der Tastenkombination "Strg+Alt+M" möglicherweise nicht das Zugriffstastenmenü aufgerufen. Diese Situation tritt bei der folgenden Clientkonfiguration auf: Fedora® Core 6 und Firefox® 1.5 oder 2.0.

Durch Tests wurde festgestellt, dass die Fensterfokussierungsprobleme bei Fedora Core 6 durch die Installation von libXp behoben werden können. Bei den von Raritan durchgeführten Tests mit libXp-1.0.0.8.i386.rpm konnten alle Probleme der Tastaturfokussierung und mit Popup-Menüs behoben werden.

Hinweis: libXp ist auch für den SeaMonkey-Browser (ehemals Mozilla®) erforderlich, damit dieser mit dem Java™-Plug-in funktioniert.

VKC- und MPC-Smart Card-Verbindungen zu Fedora-Servern

Wenn Sie eine Smart Card verwenden, um eine Verbindung zu einem Fedora®-Server über den MPC oder VKC herzustellen und Sie entnehmen die Karte, nachdem die Verbindung hergestellt wurde, ist die PCSC-Lite-Bibliothek auf den FC7- und FC8-Servern nicht freigegeben. Sie müssen den PCSC-Daemon neu starten, um diese freizugeben. Um dies zu umgehen, aktualisieren Sie die PCSC-Lite-Bibliothek auf die Version 1.4.102-3 oder höher.



Lösen von Problemen mit dem Einfrieren von Firefox bei der Benutzung von Fedora

Wenn Sie Firefox® verwenden und einen Fedora®-Server nutzen, ist es möglich, dass Firefox beim Öffnen einfriert. Um dieses Problem zu lösen, installieren Sie das Java™-Plug-in libnpjp2.so auf dem Server.

Videomodi und Auflösungen

Videomodi für SUSE/VESA

Das SuSE X.org-Konfigurationstool "SaX2" erzeugt Videomodi mithilfe von Modeline-Einträgen in der X.org-Konfigurationsdatei. Diese Videomodi stimmen nicht exakt mit der Zeitabstimmung des VESA-Videomodus überein (auch wenn ein VESA-Monitor ausgewählt wurde). Dominion KX II verwendet die Zeitabstimmung des VESA-Videomodus für die ordnungsgemäße Synchronisierung und verlässt sich auf deren Richtigkeit. Diese Unstimmigkeit kann zu schwarzen Rändern, fehlenden Abschnitten im Bild und Rauschen führen.

► **So konfigurieren Sie die SUSE-Videoanzeige:**

1. Die erzeugte Konfigurationsdatei "/etc/X11/xorg.conf" enthält einen Abschnitt zum Monitor mit einer Option, die als "UseModes" bezeichnet wird, z. B.
   UseModes "Modes[0]".
2. Kommentieren Sie diese Zeile aus (mit #) oder löschen Sie sie vollständig.
3. Starten Sie den X-Server neu.

Durch diese Änderung wird die interne Zeitabstimmung für den Videomodus des X-Servers verwendet, der exakt mit der Zeitabstimmung des VESA-Videomodus übereinstimmt und so zur gewünschten Videoanzeige auf Dominion KX II führt.

Unterstützte Videoauflösungen, die nicht angezeigt werden

Wenn Sie ein CIM verwenden, gibt es einige Videoauflösungen, wie unter ***Unterstützte Videoauflösungen*** (auf Seite 323) aufgelistet, die nicht standardmäßig zur Auswahl stehen.

► **So können Sie alle verfügbaren Videoauflösungen anzeigen:**

1. Stecken Sie den Monitor ein.
2. Stecken Sie als nächsten Schritt den Monitor wieder aus und das CIM ein. Jetzt sind alle Videoauflösungen verfügbar und können verwendet werden.



USB-Ports und -Profile

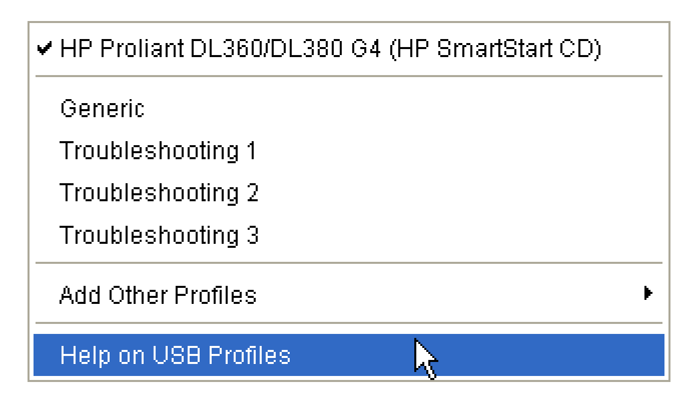
VM-CIMs und DL360 USB-Ports

HP® DL360-Server verfügen über einen USB-Port auf der Rückseite des Geräts und einen weiteren auf der Vorderseite. Mit DL360 können nicht beide Ports gleichzeitig verwendet werden. Deshalb kann ein duales VM-CIM auf DL360-Servern nicht verwendet werden.

Sie können jedoch einen USB2-Hub an den USB-Port auf der Rückseite des Geräts angeschlossen werden, an den wiederum ein duales VM-CIM angeschlossen werden kann.

Hilfe bei der Auswahl von USB-Profilen

Wenn Sie im VKC mit einem KVM-Zielserver verbunden sind, können Sie Informationen zu USB-Profilen über den Befehl "Help on USB Profiles" (Hilfe bei USB-Profilen) im Menü "USB Profile" (USB-Profil) anzeigen.



Das Fenster "USB Profile Help" (Hilfe für USB-Profile) wird angezeigt. Weitere Informationen zu speziellen USB-Profilen finden Sie unter ***Verfügbare USB-Profile*** (auf Seite 119).

Raritan stellt eine Standardauswahl an USB-Konfigurationsprofilen für eine große Anzahl an Serverimplementierungen für Betriebssysteme und auf BIOS-Ebene an. Diese sorgen für optimale Übereinstimmung bei Konfigurationen von Remote-USB-Geräten und Zielservern.

Das Profil "Generic" (Generisch) erfüllt die Anforderungen der meisten häufig bereitgestellten Zielserverkonfigurationen.

Weitere Profile stehen zur Verfügung, um die speziellen Anforderungen anderer häufig bereitgestellten Serverkonfigurationen (z. B. Linux® und Mac OS-X®) zu erfüllen.

Außerdem stehen einige Profile (festgelegt nach Plattformname und BIOS-Revision) zur Verfügung, die erstellt wurden, um die Kompatibilität der Funktion der virtuellen Medien mit dem Zielserver zu verbessern (wenn z. B. auf BIOS-Ebene gearbeitet wird).

Mit "Add Other Profiles" (Weitere Profile hinzufügen) haben Sie Zugriff auf andere auf dem System verfügbare Profile. Aus dieser Liste ausgewählte Profile werden zum Menü "USB Profile" (USB-Profil) hinzugefügt. Dazu gehört eine Reihe von Problembehebungsprofilen, mit denen Sie Konfigurationsbeschränkungen ermitteln können.

Sie ausgewählten Profile im Menü "USB Profile" (USB-Profil) sind unter "Console Device Settings" > "Port Configuration" (Konsolengeräteeinstellungen > Portkonfiguration) konfigurierbar.

Sollte keines der Standard-USB-Profile von Raritan Ihren Zielserveranforderungen entsprechen, können Sie zusammen mit dem technischen Kundendienst von Raritan eine den Anforderungen Ihres Zielgeräts entsprechende Lösung erarbeiten. Raritan empfiehlt, Folgendes zu überprüfen:

1. Überprüfen Sie die neuesten Versionshinweise auf der Seite "Firmware Upgrade" (Firmwareaktualisierung) der Raritan-Website (www.raritan.com), um festzustellen, ob für Ihre Konfiguration bereits eine Lösung verfügbar ist.
2. Wenn dies nicht der Fall ist, stellen Sie die folgenden Informationen zur Verfügung, wenn Sie sich an den technischen Kundendienst von Raritan wenden:
   a. Zielserverinformationen, Hersteller, Modell, BIOS, Hersteller und Version
   b. Verwendungszweck (z. B. Umleiten eines Abbildes, um das Betriebssystem eines Servers von CD neu zu laden)



Ändern eines USB-Profils bei Verwendung eines Smart Card-Lesegeräts

Unter bestimmten Umständen kann es erforderlich sein, das USB-Profil für einen Zielserver zu ändern. Zum Beispiel wenn Sie bei Problemen des Ziels mit der USB-Hochgeschwindigkeitsverbindung die Verbindungsgeschwindigkeit auf "Use Full Speed for Virtual Media CIM" (Volle Geschwindigkeit für virtuelles Medien-CIM verwenden) ändern möchten.

Nachdem ein Profil geändert wurde, erhalten Sie die Meldung "New Hardware Detected" (Neue Hardware gefunden) und werden aufgefordert, sich mit Administratorberechtigung am Ziel anzumelden, um den USB-Treiber erneut zu installieren. Meistens geschieht dies nur die ersten Male, wenn das Ziel die neuen Einstellungen für das USB-Gerät erkennt. Danach wählt das Ziel den richtigen Treiber aus.

CIMs

Windows-3-Tasten-Maus auf Linux-Zielgeräten

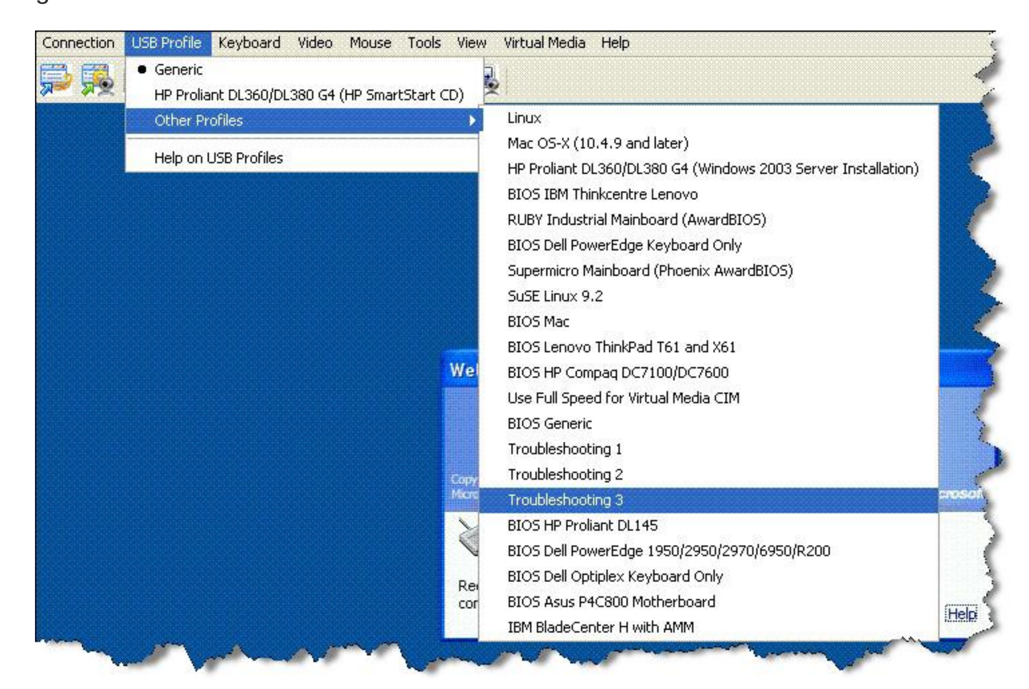
Wenn Sie auf einem Windows®-Client eine 3-Tasten-Maus verwenden und eine Verbindung zu einem Linux®-Zielgerät herstellen, wird die linke Maustaste möglicherweise der mittleren Taste der 3-Tasten-Maus des Windows-Client zugeordnet.

Composite-USB-Geräteverhalten bei virtuellen Medien auf Windows 2000

Das Betriebssystem Windows 2000® unterstützt Composite-USB-Geräte (z. B. D2CIM-VUSB von Raritan) nicht im gleichen Maße wie Non-Composite-USB-Geräte.

Aus diesem Grund wird das Symbol zum sicheren Entfernen der Hardware im Infobereich der Taskleiste bei Laufwerken, die von D2CIM-VUSB zugeordnet wurden, nicht angezeigt, und beim Verbinden des Geräts wird möglicherweise eine Warnmeldung angezeigt. Es wurden von Raritan jedoch keine daraus resultierenden Probleme oder Fehler festgestellt.

Die Entwicklungsabteilung von Raritan in den USA hat eine Konfiguration entwickelt, die das Symbol zum sicheren Entfernen der Hardware unterstützt und die Warnmeldung unterdrückt. Um diese Konfiguration nutzen zu können, müssen Sie den D2CIM-DVUSB-Adapter für virtuelle Medien sowie das USB-Profil "Troubleshooting 3" (Fehlerbehebung 3) verwenden, wodurch D2CIM-DVUSB als Non-Composite-USB-Gerät mit Unterstützung für eine einzelne virtuelle Medienverbindung konfiguriert wird. Diese Konfiguration wurde von Raritan in den USA und Japan erfolgreich getestet.





Virtual Media (Virtuelle Medien)

Virtuelle Medien werden nach dem Hinzufügen von Dateien nicht aktualisiert

Nach der Installation eines virtuellen Medienlaufwerks werden dem Laufwerk hinzugefügte Dateien möglicherweise nicht unmittelbar auf dem Zielserver angezeigt. Trennen Sie die virtuelle Medienverbindung und stellen Sie sie erneut her.

Zugriff auf virtuelle Medien auf einem Windows 2000 Server mithilfe eines D2CIM-VUSB

Der Zugriff auf virtuelle Medien auf einem lokalen Laufwerk auf einem Windows 2000® Server ist mit D2CIM-VUSB nicht möglich.

Bootzeit des Ziel-BIOS bei Verwendung von virtuellen Medien

Das BIOS bestimmter Zielgeräte benötigt möglicherweise mehr Zeit zum Hochfahren, wenn virtuelle Medien auf dem Zielgerät installiert sind.

► **So verkürzen Sie die Bootzeit:**

1. Schließen Sie den Virtual KVM Client, sodass die virtuellen Medienlaufwerke vollständig freigegeben werden.
2. Starten Sie das Zielgerät neu.

Fehler bei Hochgeschwindigkeitsverbindungen mit virtuellen Medien

Unter bestimmten Umständen kann es erforderlich sein, die Verbindungsgeschwindigkeit "Use Full Speed for Virtual Media CIM" (Volle Geschwindigkeit für virtuelles Medien-CIM verwenden) auszuwählen. Zum Beispiel bei Problemen des Ziels mit der USB-Hochgeschwindigkeitsverbindung oder wenn beim Ziel USB-Protokollfehler aufgrund von Signalstörungen, zusätzlichen Anschlüssen und Kabeln (z. B. eine Verbindung zu einem Bladeserver über Dongle) auftreten.



CC-SG

Version des Virtual KVM Client im CC-SG-Proxymodus nicht bekannt

Wenn der Virtual KVM Client über CommandCenter Secure Gateway (CC-SG) im Proxymodus gestartet wird, ist die Version des Virtual KVM Client unbekannt. Im Dialogfeld "About Raritan Virtual KVM Client" (Informationen zum Raritan Virtual KVM Client) wird die Version als "Version Unknown" (Version unbekannt) angezeigt.

Ein-Cursor-Modus – Verbinden mit einem Dominion KX II-Zielgerät unter CC-SG-Steuerung über VKC und Verwendung von Firefox

Wenn Sie Firefox® nutzen, um eine Verbindung zu einem Dominion KX II-Zielgerät unter CC-SG-Steuerung herzustellen, und DCIM-PS2 oder DCIM-USBG2 verwenden, erscheint das VKC-Fenster nicht mehr als Fokusfenster, wenn Sie im Virtual KVM Client in den Ein-Cursor-Modus wechseln, und die Maus reagiert nicht mehr. Drücken Sie in diesem Fall die linke Maustaste oder die Alt-+Tab-Taste, um den Fokus auf das VKC-Fenster zurückzuschalten.

Proxymodus und MPC

Wenn Sie Dominion KX II in einer CC-SG-Konfiguration verwenden, sollten Sie den CC-SG-Proxymodus nicht verwenden, wenn Sie den Multi-Platform-Client (MPC) nutzen möchten.

Wechseln zwischen Dominion KX II-Ports

Wenn Sie zwischen Ports desselben Dominion KX II-Geräts wechseln und die Verwaltung innerhalb von einer Minute wieder aufnehmen, zeigt CC-SG möglicherweise eine Fehlermeldung an. Die Anzeige wird aktualisiert, wenn Sie die Verwaltung wieder aufnehmen.



Anhang D Häufig gestellte Fragen (FAQs)

In diesem Kapitel



Allgemeine Fragen

Was ist Dominion KX II?

Dominion KX II ist ein digitaler KVM-Switch (Tastatur, Video, Maus) der zweiten Generation, der einem, zwei, vier oder acht IT-Administrator(en) den Zugriff auf 8, 16, 32 oder 64 Server und deren Steuerung über das Netzwerk mit Funktionen auf BIOS-Ebene erlaubt. Dominion KX II ist vollständig unabhängig von Hardware und Betriebssystem. Benutzer können Fehler am Server beheben und diesen neu konfigurieren, auch wenn er nicht verfügbar ist.

Im Serverschrank montiert bietet die platzsparende Dominion KX II-Einheit die gleiche Funktionalität, den gleichen Bedienkomfort und die gleiche Kostenersparnis wie herkömmliche KVM-Switches. Dominion KX II verfügt jedoch auch über die leistungsfähigste KVM-über-IP-Technologie der Branche, die mehreren Administratoren den Zugriff auf Server-KVM-Konsolen über eine beliebige vernetzte Workstation ermöglicht.

Was unterscheidet Dominion KX II von Software zur Remotesteuerung?

Bei der Remoteverwendung von Dominion KX II erscheint die Benutzeroberfläche zunächst ähnlich der von Software zur Remotesteuerung wie pcAnywhere, Windows Terminal Services/Remote Desktop, VNC usw. Da Dominion KX II jedoch keine Software-, sondern eine Hardwarelösung ist, ist das Gerät wesentlich leistungsstärker. Dies gilt speziell für folgende Merkmale:

- Betriebssystem- und hardwareunabhängig – Dominion KX II kann zur Verwaltung von Servern mit vielen beliebten Betriebssystemen verwendet werden. Dazu zählen Intel®, Sun™, PowerPC mit Windows®, Linux®, Solaris™, etc.
- Statusunabhängig/Agent-frei – Dominion KX II erfordert nicht, dass das Betriebssystem des verwalteten Servers ausgeführt wird oder dass auf dem verwalteten Server spezielle Software installiert ist.
- Out-of-Band – Auch wenn die Netzwerkverbindung des verwalteten Servers nicht verfügbar ist, kann der Server dennoch mit Dominion KX II verwaltet werden.
- Zugriff auf BIOS-Ebene – Dominion KX II funktioniert auch dann fehlerfrei und ermöglicht die erforderlichen Konfigurationen, wenn der Server nicht hochfährt, im abgesicherten Modus gestartet werden muss oder wenn seine BIOS-Parameter geändert werden müssen.

Welche neuen Features hat Dominion KX II im Vergleich zum KX I?



Dominion KX II bietet viele interessante neue Funktionen. Dazu gehören virtuelle Medien, den Mausmodus "Absolute Mouse Synchronization™", zwei Netzteile, duales Gigabit-Ethernet, allgemeine webbasierte Benutzeroberflächen, einen lokalen Port der nächsten Generation und vieles mehr.

Wie funktioniert die Migration von Dominion KX I auf Dominion KX II?

Grundsätzlich können Sie als Kunde Ihre vorhandenen Switches noch viele Jahre nutzen. Wenn Ihr Rechenzentrum wächst, können Sie die neuen Dominion KX II-Modelle erwerben und einsetzen. Die zentrale Verwaltungseinheit von Raritan, CommandCenter Secure Gateway, und der Multi-Platform-Client (MPC) unterstützen sowohl KX I- als auch Dominion KX II-Switches nahtlos.

Funktionieren meine bisherigen KX I-CIMs mit den Dominion KX II-Switches?

Ja, vorhandene KX I-CIMs funktionieren mit dem Dominion KX II-Switch. Darüber hinaus können auch ausgewählte Paragon-CIMs für Dominion KX II eingesetzt werden. Dies erleichtert es Paragon I-Kunden, die zu KVM-über-IP wechseln möchten, die Migration zu Dominion KX II. Sie sollten jedoch auch die CIMs D2CIM-VUSB und D2CIM-DVUSB in Erwägung ziehen, die virtuelle Medien und den Mausmodus "Absolute Mouse Synchronization" unterstützen.

Kann Dominion KX II in einem Gestell montiert werden?

Ja. Dominion KX II wird standardmäßig mit 19-Zoll-Gestellhalterungen geliefert. Er kann auch umgekehrt im Gestell montiert werden, sodass die Serverports nach vorne zeigen.

Wie groß ist Dominion KX II?

Das Dominion KX II-Gerät ist nur 1U hoch (mit Ausnahme der Modelle KX2-864 und KX2-464, welche 2U hoch sind), passt in ein 19-Zoll-Standardgestell und ist nur 29 cm tief. Die Modelle Dominion KX2-832 und KX2-864 sind 44 cm tief.



Remotezugriff

Wie viele Benutzer können bei einem Dominion KX II-Gerät von einem Remotestandort aus auf Server zugreifen?

Die Dominion KX II-Modelle bieten bis zu acht Benutzern pro Kanal Remoteverbindungen für den gleichzeitigen Zugriff auf einen einzelnen Zielserver und dessen Steuerung. Bei Ein-Kanal-Geräten wie dem DKX2-116 können bis zu acht Remotebenutzer auf einen einzelnen Zielserver zugreifen und diesen steuern. Bei Zwei-Kanal-Geräten wie dem DKX2-216 können bis zu acht Benutzer auf Kanal eins auf den Server zugreifen und diesen steuern, und weiteren acht Benutzern steht Kanal zwei zur Verfügung. Bei Vier-Kanal-Geräten können bis zu acht Benutzer pro Kanal auf vier Server zugreifen und diese steuern. Dies ergibt insgesamt 32 (8 x 4) Benutzer. Bei Acht-Kanal-Geräten können bis zu acht Benutzer auf einen einzelnen Server zugreifen. Insgesamt können dabei maximal 32 Benutzer die 8 Kanäle verwenden.

Können zwei Personen gleichzeitig denselben Server anzeigen?

Ja, bis zu acht Personen können gleichzeitig auf einen einzelnen Server zugreifen und diesen steuern.

Können zwei Personen auf denselben Server zugreifen (einer an einem Remotestandort und einer über den lokalen Port)?

Ja, der lokale Port ist vollständig unabhängig von den Remote-"Ports". Über den lokalen Port können sie mithilfe des PC-Freigabe-Features auf denselben Server zugreifen.

Welche Hardware-, Software- oder Netzwerkkonfiguration ist für den Zugriff auf Dominion KX II über einen Client erforderlich?

Da Dominion KX II über das Web verfügbar ist, muss auf Clients keine spezielle Software für den Zugriff installiert werden. Für den Zugriff über externe Modems ist ein optionaler Client unter "Raritan.com" verfügbar.

Der Zugriff auf Dominion KX II ist über Webbrowser möglich. Hierzu zählen: Internet Explorer und Mozilla Firefox. Sie können ab sofort über den neuen Windows Client von Raritan, die Java-basierte Multiplattform und Virtual KVM Client über Windows-, Linux- und Macintosh-Desktop-Computer auf Dominion KX II zugreifen.

Dominion KX II-Administratoren können mithilfe einer praktischen browserbasierten Oberfläche Remote-Verwaltungsfunktionen, wie das Einrichten von Passwörtern und Sicherheitseinstellungen, das Umbenennen von Servern, das Ändern von IP-Adressen usw., ausführen.

Wie groß sind die Dateien des Virtual KVM Client-Applets, das für den Zugriff auf Dominion KX II verwendet wird? Wie lange dauert das Herunterladen?



Das Virtual KVM Client-Applet für den Zugriff auf Dominion KX II ist etwa 500 KB groß. Die folgende Tabelle zeigt, wie lange das Herunterladen des Dominion KX II-Applets bei verschiedenen Netzwerkgeschwindigkeiten dauert:

Geschwindigkeit	Beschreibung	Dauer
100 Mbit/s	Theoretisch 100 Mbit	0,05 Sekunden
60 Mbit/s	Beinahe 100 Mbit	0,08 Sekunden
10 Mbit/s	Theoretisch 10 Mbit	0,4 Sekunden
6 Mbit/s	Beinahe 10 Mbit	0,8 Sekunden
512 Kbit/s	Kabelmodem-Downloadgeschwindigkeit (normal)	8 Sekunden

Wie greife ich auf die an Dominion KX II angeschlossenen Server zu, wenn das Netzwerk nicht verfügbar ist?

Sie können am Serverschrank oder über Modem auf Server zugreifen. Dominion KX II besitzt einen dedizierten Modemport für den Anschluss eines externen Modems.

Haben Sie einen Windows®-Client?

Ja, Version 2.2 verfügt über einen Native .NET-Windows-Client, den Raritan Active KVM Client.

Gibt es einen Client für andere Betriebssysteme als Windows?

Ja. Sowohl der Virtual KVM Client als auch der Multi-Platform-Client (MPC) ermöglichen es Benutzern, die nicht über ein Windows-Betriebssystem verfügen, über die Dominion KX I- und Dominion KX II-Switches Verbindungen mit den KVM-Zielservern herzustellen. MPC kann über Webbrowser oder als eigenständige Version betrieben werden. Weitere Informationen finden Sie unter **Virtual KVM Client** und **Raritan Multi-Platform Client (MPC) Supported Operating Systems** im Benutzerhandbuch **KVM and Serial Client Guide**.

Unterstützen Ihre KVM-Clients LCD-Monitore?

Ja. Für Kunden, die ihre Produktivität mithilfe mehrerer LCD-Monitore auf dem Schreibtisch verbessern möchten, kann Dominion KX II KVM-Sitzungen auf mehreren Monitoren im Vollbild- oder in Standardmodi starten.

Während einer Sitzung des Virtual KVM Client klemmt manchmal die Alt-Taste. Was kann ich in diesem Fall tun?

Dieses Problem kann auftreten, wenn die Alt-Taste gedrückt und nicht losgelassen wird. Wenn bei gedrückter Alt-Taste z. B. die Leertaste gedrückt wird, kann der Fokus vom Zielserver zum Client-PC wechseln. Das lokale Betriebssystem interpretiert diese Tastenkombination und löst die Aktion für die Tastenkombination im aktiven Fenster aus (auf dem Client-PC).



Universelle virtuelle Medien

Welche <ProductName<-Modelle unterstützen virtuelle Medien?

Alle Dominion KX II-Modelle unterstützen virtuelle Medien. Sie sind als eigenständige Angebote oder im Rahmen von CommandCenter Secure Gateway, der zentralen Verwaltungseinheit von Raritan, verfügbar.

Welche Arten von virtuellen Medien unterstützt Dominion KX II?

Folgende Medienarten werden von Dominion KX II unterstützt: interne und per USB angeschlossene CD- und DVD-Laufwerke, USB-Massenspeichergeräte, PC-Festplatten und ISO-Abbilder.

Welche Voraussetzungen müssen für virtuelle Medien erfüllt sein?

Ein Dominion KX II-CIM für virtuelle Medien ist erforderlich. Von diesen CIMs gibt es zwei Arten: das D2CIM-VUSB und das neue D2CIM-DVUSB.

Das D2CIM-DVUSB besitzt zwei USB-Anschlüsse und sollte von Kunden erworben werden, die virtuelle Medien auf BIOS-Ebene einsetzen möchten. Das D2CIM-DVUSB ist ebenfalls für die Smart Card-Authentifizierung erforderlich.

Das D2CIM-VUSB besitzt einen USB-Anschluss und ist für Kunden gedacht, die virtuelle Medien auf Betriebssystemebene verwenden.

Beide unterstützen virtuelle Mediensitzungen mit Zielservern, die über eine USB 2.0-Schnittstelle verfügen.

Diese CIMs sind in günstigen Paketen zu 32 oder 64 Stück verfügbar und unterstützen den Mausmodus "Absolute Mouse Synchronization" (Absolute Maussynchronisierung) sowie die Remote-Firmwareaktualisierung.

Sind virtuelle Medien sicher?

Ja. Virtuelle Mediensitzungen werden durch eine AES- oder -RC4-Verschlüsselung abgesichert.

USB-Profile

Was ist ein USB-Profil?

Bestimmte Server benötigen eine speziell konfigurierte USB-Schnittstelle für USB-basierte Dienste wie virtuelle Medien. Durch die USB-Profile wird die USB-Schnittstelle des Dominion KX II auf den Server abgestimmt, sodass sie den speziellen Eigenschaften des Servers entspricht.

Warum sollte ich ein USB-Profil verwenden?

USB-Profile sind meistens auf BIOS-Ebene erforderlich, wo möglicherweise keine vollständige Unterstützung für die USB-Spezifikation beim Zugriff auf virtuelle Medienlaufwerke besteht.

Profile werden jedoch manchmal auch auf Betriebssystemebene verwendet, z. B. für die Maussynchronisierung bei Mac® und Linux®-Servern.

Wie wird ein USB-Profil verwendet?

Auf den Seiten zur Dominion KX II-Portkonfiguration können individuelle oder Gruppen von Ports vom Administrator konfiguriert werden, sodass ein spezielles USB-Profil verwendet wird.

Ein USB-Profil kann ggf. auch im Dominion KX II-Client ausgewählt werden.

Was passiert, wenn ich ein falsches USB-Profil auswähle?

Wenn Sie ein falsches USB-Profil für einen KVM-Zielserver auswählen, kann dies dazu führen, dass ein Massenspeichergerät, eine Maus oder eine Tastatur nicht optimal oder gar nicht funktioniert.

Muss ich immer ein USB-Profil verwenden, wenn ich virtuelle Medien nutze?

Nein, in vielen Fällen reicht das Standard-USB-Profil bei der Verwendung von virtuellen Medien auf Betriebssystemebene oder bei Vorgängen auf BIOS-Ebene ohne Zugriff auf virtuelle Medien aus.

Welche Profile stehen zur Verfügung?

Siehe ***Verfügbare USB-Profile*** (auf Seite 119).

Woher weiß ich, welches USB-Profil für einen Zielserver am besten geeignet ist?

Das generische Profi ist für die große Mehrheit an Zielservern am besten geeignet. Wenn dieses Profil bei einem bestimmten KVM-Zielserver nicht funktioniert, können Sie das entsprechende USB-Profil unter ***Verfügbare USB-Profile*** (auf Seite 119) auswählen. Wählen Sie das Profil aus, das Ihrem Zielserver am besten entspricht.



Worin besteht der Zweck eines BIOS-Profils?

Ein BIOS-Profil wurde auf die Anforderungen eines bestimmten Server-BIOS, das die vollständige USB-Spezifikation nicht erfüllt, abgestimmt. Mit dem Profil können Tastatur, Maus und virtuelle Medien auf BIOS-Ebene verwendet und so die Beschränkungen des BIOS umgangen werden.

Benötige ich ein spezielles CIM, um USB-Profile nutzen zu können?

Sie müssen ein D2CIM-VUSB oder D2CIM-DVUSB mit aktualisierter Firmware verwenden.

Stellt Raritan USB-Profile für andere Zielserverkonfigurationen zur Verfügung?

Raritan stellt neue USB-Profile zur Verfügung, die den Kundenanforderungen entsprechen. Wenn diese Profile verfügbar sind, werden sie den Firmwareaktualisierungen beigefügt.

Bandbreite und KVM-über-IP-Leistung

Wie wird in KVM-über-IP-Systemen die Bandbreite genutzt?

Dominion KX II verfügt über die KVM-über-IP-Technologie der nächsten Generation – und damit über die beste derzeit verfügbare Videokomprimierung. Raritan hat für die hohe Qualität der Videoübertragung und die niedrige Auslastung der Bandbreite zahlreiche Auszeichnungen erhalten.

Dominion KX II digitalisiert, komprimiert und verschlüsselt die Tastatur-, Video- und Maussignale des Zielservers und übermittelt IP-Pakete über das IP-Netzwerk an den Remoteclient, um die Remotesitzung für den Benutzer herzustellen. Durch die branchenführenden Videoverarbeitungs-Algorithmen des Dominion KX II haben Sie das Gefühl, direkt am Serverschrank zu arbeiten.

Bildwechsel (z. B. bei Videoanzeigen) benötigen den größten Teil der verwendeten Bandbreite, während Tastatur- und Mausaktivitäten wesentlich weniger verbrauchen.

Beachten Sie, dass Bandbreite nur genutzt wird, wenn der Benutzer aktiv ist. Wie viel Bandbreite genutzt wird, hängt von der Anzahl der Bildwechsel auf dem Server ab.

Wenn keine Bildwechsel stattfinden (der Benutzer also nicht mit dem Server interagiert), wird normalerweise keine Bandbreite genutzt. Wenn der Benutzer die Maus bewegt oder ein Zeichen eingibt, wird eine geringe Menge an Bandbreite genutzt. Wenn auf dem Bildschirm ein komplexer Bildschirmschoner oder ein Video läuft, erhöht sich die genutzte Bandbreite.

Welche Auswirkungen hat die Bandbreite auf die KVM-über-IP-Leistung?

Generell hängen Bandbreite und Leistung zusammen. Je mehr Bandbreite verfügbar ist, desto besser kann die Leistung sein. In Umgebungen mit eingeschränkter Bandbreite kann die Leistung verringert werden. Dominion KX II wurde so entwickelt, dass bei einer großen Anzahl verschiedener Umgebungen sehr gute Leistung erzielt wird.

Welche Faktoren beeinträchtigen die Bandbreite?

Wie viel Bandbreite genutzt wird, hängt von mehreren Faktoren ab. Der primäre Faktor ist, wie oben beschrieben, die Anzahl der Bildwechsel auf dem Zielserver. Diese hängt von den Aufgaben und Aktionen des Benutzers ab.

Zu den anderen Faktoren zählen Videoauflösung des Servers, Netzwerkgeschwindigkeit und -eigenschaften, Ressourcen des Client-PC sowie Rauschen der Grafikkarte.



Dominion KX II verfügt über hoch entwickelte Videoverarbeitungs-Algorithmen, durch die Bandbreite und Leistung für viele Umgebungen optimiert werden. Außerdem sind diese durch viele Einstellungsmöglichkeiten zur Optimierung der Bandbreitennutzung in hohem Maße konfigurierbar. So kann beispielsweise die Verbindungsgeschwindigkeit für die Remoteclients (VKC, MPC) so eingestellt werden, dass weniger Bandbreite genutzt wird.

Im Gegensatz zum KX I hat der Rauschfilterparameter hier normalerweise keinen großen Einfluss auf die Verringerung der Bandbreite oder die Verbesserung der Leistung.

Wie viel Bandbreite verwendet KX II für allgemeine Aufgaben?

Die Bandbreitennutzung hängt primär von den Aufgaben und Aktionen des Benutzers ab. Je mehr Bildwechsel, desto höher die erforderliche Bandbreite.

In der folgenden Tabelle werden einige Standardfälle unter Verwendung der Standard-Bandbreiteneinstellung von Dominion KX II und zwei Einstellungen mit verringerter Bandbreitennutzung (Verbindungsgeschwindigkeit 1 Mbit mit 15- und 8-Bit-Farbe) auf einem Windows XP-Zielserver (Auflösung 1024 x 768) über ein LAN mit 100 Mbit/s dargestellt:

Benutzeraufgabe	Standard	1 Mbit Geschwindigkeit & 15-Bit-Farbe	1 Mbit Geschwindigkeit & 8-Bit-Farbe
Windows-Desktop im Standbymodus	0 KB/s	0 KB/s	0 KB/s
Bewegung des Cursors	5-15 KB/s	2-6 KB/s	2-3 KB/s
Verschieben eines Symbols	40-70 KB/s	10-25 KB/s	5-15 KB/s
Verschieben eines Ordners	10-40 KB/s	5-20 KB/s	5-10 KB/s
Öffnen eines Textfensters	50-100 KB/s	25-50 KB/s	10-15 KB/s
Dauerhaftes Schreiben auf der Tastatur	1 KB/s	0,5-1 KB/s	0,2-5 KB/s
Verwenden des Bildlaufs bei Textfenstern	10-50 KB/s	5-25 KB/s	2-10 KB/s
Schließen eines Textfensters	50-100 KB/s	20-40 KB/s	10-15 KB/s

Benutzeraufgabe	Standard	1 Mbit Geschwindigkeit & 15-Bit-Farbe	1 Mbit Geschwindigkeit & 8-Bit-Farbe
Öffnen eines Feldes	50-100 KB/s	60-70 KB/s	20-30 KB/s
Wechseln der Registerkarte in einem Feld	40-50 KB/s	20-50 KB/s	10-20 KB/s
Schließen eines Feldes	50-100 KB/s	40-60 KB/s	20-30 KB/s
Ändern einer Feldoption	2-10 KB/s	1-5 KB/s	1-3 KB/s
Öffnen einer Browserseite	100-300 KB/s	50-200 KB/s	40-80 KB/s
Verwenden des Bildlaufs im Browser	75-200 KB/s	50-200 KB/s	30-100 KB/s
Schließen des Browsers	100-150 KB/s	75-100 KB/s	30-60 KB/s
Öffnen des Startmenüs	75-100 KB/s	50-75 KB/s	20-30 KB/s
Schließen des Startmenüs	75-100 KB/s	25-50 KB/s	10-15 KB/s
Bildschirmschoner Starfield	25-50 KB/s	10-15 KB/s	7-10 KB/s
Bildschirmschoner 3D-Rohre	10-100 KB/s	5-20 KB/s	2-10 KB/s
Windows-Medienvideo	500-1200 KB/s	300-500 KB/s	150-300 KB/s
QuickTime-Video 1	700-2500 KB/s	400-500 KB/s	150-350 KB/s
QuickTime-Video 2	1500-2500 KB/s	400-550 KB/s	200-350 KB/s



Mit der Einstellung für verringerte Bandbreite wird die Bandbreite bei fast allen Aufgaben deutlich reduziert. Bei der 15-Bit-Farbeinstellung ist die wahrgenommene Leistung ähnlich der mit Standardparametern. Weitere Bandbreitenreduktionen sind durch zusätzliche Änderungen der Einstellungen möglich.

Beachten Sie, dass diese Darstellungen der Bandbreite nur Beispiele sind und aufgrund von verschiedenen Faktoren von den Werten in Ihrer Umgebung abweichen können.

Wie kann ich die Bandbreite verringern?

Dominion KX II bietet verschiedene Einstellungen für die Remoteclients, um Bandbreite und Leistung zu optimieren. Die Standardeinstellungen bieten Leistung auf Serverschrankebene in Standard-LAN-/WAN-Umgebungen bei sparsamer Nutzung der Bandbreite.

Zu den Einstellungen der Bandbreitenverwaltung zählen die Verbindungsgeschwindigkeit und die Farbtiefe. So reduzieren Sie die Bandbreite:

Verbindungsgeschwindigkeit verringern

Durch die Verringerung der Verbindungsgeschwindigkeit kann die genutzte Bandbreite deutlich reduziert werden. In Standard-LAN-/WAN-Umgebungen kann durch Ändern der Verbindungsgeschwindigkeit auf 1,5 oder 1Mbit pro Sekunde die Bandbreite reduziert und gleichzeitig eine gute Leistung beibehalten werden. Durch niedrigere Einstellungen wird die Bandbreite weiter reduziert. Diese Einstellungen sind für Verknüpfungen mit langsamer Bandbreite geeignet.

Farbtiefe verringern

Durch die Verringerung der Farbtiefe wird die Bandbreite ebenso deutlich reduziert und die Leistung verbessert. Es werden jedoch weniger Farben verwendet, wodurch eine Verringerung der Videoqualität entsteht. Bei bestimmten Systemverwaltungsaufgaben ist dies möglicherweise vertretbar.

Bei langsamen Internetverbindungen kann durch Verwendung von 8-Bit-Farbtiefen oder darunter die Bandbreite verringert und die Leistung verbessert werden.

Zu den weiteren Tipps für die Verringerung der Bandbreite zählen:

- Verwendung eines einfarbigen Hintergrunds anstatt eines komplexen Bildes
- Deaktivierung des Bildschirmschoners
- Verwendung einer niedrigeren Auflösung auf dem Zielserver

- Deaktivierung der Option "Show window contents while dragging" (Fensterinhalte beim Verschieben anzeigen) in Windows
- Verwendung von einfachen Bildern, Motiven und Desktops (z. B. Windows Classic)

Was mache ich bei Verknüpfungen mit langsamer Bandbreite?

Verbindungsgeschwindigkeit und Farbtiefe können so eingestellt werden, dass die Leistung für langsamere Bandbreiten optimiert wird. Sie können die Verbindungsgeschwindigkeit im Multi-Platform-Client oder Virtual KVM Client auf 1,5 MB oder 1 MB und die Farbtiefe auf 8 Bit stellen. In Situationen mit sehr niedriger Bandbreite können auch noch niedrigere Verbindungsgeschwindigkeiten und Farbtiefen gewählt werden.

Ich möchte eine Verbindung über das Internet herstellen. Welche Art von Leistung kann ich erwarten?

Dies hängt von der Bandbreite und Latenz der Internetverbindung zwischen Ihrem Remoteclient und Dominion KX II ab. Mit einer Verbindung über Kabelmodem oder über eine Hochgeschwindigkeits-DSL-Verbindung kann die Leistung mit der einer LAN-/WAN-Verbindung vergleichbar sein. Bei Verknüpfungen mit niedrigerer Geschwindigkeit können Sie mithilfe der oben beschriebenen Vorschläge die Leistung verbessern.

Ich verfüge über eine Umgebung mit hoher Bandbreite. Wie kann ich die Leistung optimieren?

Die Standardeinstellungen bieten in einer Umgebung mit hoher Bandbreite sehr gute Leistung. Stellen Sie sicher, dass die Verbindungsgeschwindigkeit auf 100 MB oder 1GB und die Farbtiefe auf 15-Bit-Farbe (RGB) eingestellt ist.

Welche maximale Remote-Videoauflösung (über IP) wird unterstützt?

Dominion KX II ist der erste und einzige KVM-über-IP-Switch, der eine vollständige Remote-Videoauflösung in High Definition (HD) von 1920x1080 unterstützt.

Außerdem werden beliebte Breitbildformate unterstützt, einschließlich 1600x1200, 1680x1050 und 1440x900, so dass Remote-Benutzer mit den aktuellen hochauflösenden Monitoren arbeiten können.

Was muss ich bei Servern mit DVI-Ports beachten?

Server mit DVI-Ports, die DVI-A (analog) und DVI-I (analog und digital integriert) unterstützen, können einen einfachen, passiven Adapter, wie ADVI-VGA, verwenden, um den DVI-Port in einen VGA-Stecker zu konvertieren, der an den VGA-Stecker eines Dominion KX II-CIM angeschlossen werden kann.



Server mit DVI-Ports, die nur DVI-D (digital) unterstützen, benötigen einen teureren Adapter. Sie können jedoch prüfen, ob die Videokarte des Servers für die Unterstützung von DVI-I oder DVI-A konfiguriert werden kann.

Ethernet und IP-Netzwerk

Verfügt Dominion KX II über zwei Gigabit-Ethernet-Ports für redundantes Failover?

Ja. Dominion KX II verfügt über duale Gigabit-Ethernet-Ports für redundante Failoverfunktionen. Fällt der primäre Ethernet-Port (oder der Switch/Router, an dem der Ethernet-Port angeschlossen ist) aus, verwendet Dominion KX II den sekundären Netzwerkport mit derselben IP-Adresse, wodurch sichergestellt wird, dass der Serverbetrieb nicht unterbrochen wird. Hierzu muss der Administrator jedoch das automatische Failover aktivieren.

Wie schnell sind die Ethernet-Schnittstellen des Dominion KX II?

Dominion KX II unterstützt sowohl Gigabit- als auch 10/100-Ethernet. Dominion KX II unterstützt zwei 10/100/1000-Ethernet-Schnittstellen mit konfigurierbaren Geschwindigkeits- und Duplexeinstellungen (entweder automatisch erkannt oder manuell eingestellt).

Verfügt Dominion KX II über zwei Gigabit-Ethernet-Ports für redundantes Failover oder Lastenausgleich?

Ja. Der Dominion KX II verfügt über duale Gigabit-Ethernet-Ports für redundante Failoverfunktionen. Fällt der primäre Ethernet-Port (oder der Switch/Router, an dem der Ethernet-Port angeschlossen ist) aus, verwendet der Dominion KX II den sekundären Netzwerkport mit derselben IP-Adresse, wodurch sichergestellt wird, dass der Server-betrieb nicht unterbrochen wird. Hierzu muss der Administrator jedoch das automatische Failover aktivieren.

Kann ich über eine Drahtlosverbindung auf Dominion KX II zugreifen?

Ja. Dominion KX II verwendet nicht nur das Standard-Ethernet, sondern auch eine sehr sparsame Bandbreite mit hoher Videoqualität. Wenn also ein Wirelessclient über eine Netzwerkverbindung zu Dominion KX II verfügt, können Server auf BIOS-Ebene drahtlos konfiguriert und verwaltet werden.

Kann Dominion KX II über das WAN (Internet) oder nur über das Firmen-LAN verwendet werden?

Unabhängig davon, ob die Verbindung über ein schnelles Firmen-LAN, das wenig prognostizierbare WAN (Internet), ein Kabelmodem oder ein DFÜ-Modem hergestellt wird, passt sich die KVM-über-IP-Technologie des Dominion KX II an die Verbindung an.

Kann ich Dominion KX II mit VPN verwenden?

Ja, Dominion KX II verwendet standardmäßige Internet Protocol (IP)-Technologien von Schicht 1 bis Schicht 4. Der Datenverkehr kann leicht über Standard-VPNs geleitet werden.



Kann ich Dominion KX II mit einem Proxyserver verwenden?

Ja. Dominion KX II kann mit einem SOCKS-Proxyserver verwendet werden, vorausgesetzt, der Remote-Client-PC ist entsprechend konfiguriert. Weitere Informationen finden Sie in der Benutzerdokumentation oder der Online-Hilfe.

Wie viele TCP-Ports müssen in meiner Firewall geöffnet sein, um den Netzwerkzugriff auf Dominion KX II zu ermöglichen? Sind diese Ports konfigurierbar?

Nur einer. Dominion KX II schützt das Netzwerk, indem er für seinen Betrieb nur einen einzelnen TCP-Port benötigt. Dieser Port ist vollständig konfigurierbar, was zusätzliche Sicherheit bietet.

Beachten Sie hierzu, dass zur Nutzung der optionalen Webbrowserfunktionen des Dominion KX II auch der Standard-HTTPS-Port 443 geöffnet sein muss.

Benötigt Dominion KX II einen externen Authentifizierungsserver?

Nein. Dominion KX II ist vollständig unabhängig. Nachdem Sie der Dominion KX II-Einheit eine IP-Adresse zugeordnet haben, ist diese betriebsbereit. Die Webbrowser- und Authentifizierungsfunktionen sind vollständig integriert.

Wird ein externer Authentifizierungsserver (wie LDAP, Active Directory, RADIUS usw.) verwendet, unterstützt Dominion KX II dies ebenfalls. Sollte dieser ausfallen, verwendet die Einheit seine eigene interne Authentifizierung. Dominion KX II ermöglicht die einfache Installation, die vollständige Unabhängigkeit von einem externen Server und maximale Flexibilität.

Kann Dominion KX II mit CITRIX verwendet werden?

Wenn Dominion KX II korrekt konfiguriert wurde, funktioniert er in der Regel mit Produkten für den Remotezugriff wie CITRIX; Raritan kann jedoch nicht für eine akzeptable Leistung garantieren. Produkte wie CITRIX verwenden ähnliche Technologien zur Videoumleitung wie digitale KVM-Switches. Das bedeutet, dass gleichzeitig zwei KVM-über-IP-Technologien genutzt werden.

Kann Dominion KX II DHCP verwenden?

DHCP-Adressen können zwar verwendet werden, Raritan empfiehlt jedoch die Verwendung fester Adressen, da es sich bei Dominion KX II um ein Infrastrukturgerät handelt, bei dem eine feste IP-Adresse den Zugriff und die Wartung vereinfacht.

Ich kann über mein IP-Netzwerk keine Verbindung zu Dominion KX II herstellen. Woran kann das liegen?

Dominion KX II ist auf Ihr LAN-/WAN-Netzwerk angewiesen. Folgende Probleme könnten die Ursache sein:

- Automatische Ethernet-Verhandlung – In manchen Netzwerken funktioniert die automatische 10/100-Aushandlung nicht ordnungsgemäß und die Dominion KX II-Einheit muss auf 100 MB/Vollduplex oder die für das Netzwerk zutreffende Einstellung justiert werden.
- Doppelte IP-Adresse – Wenn Dominion KX II und ein anderes Gerät dieselbe IP-Adresse haben, wird die Netzwerkverbindung möglicherweise gestört.
- Port 5000-Konflikte – Verwendet ein anderes Gerät den Port 5000, muss der Dominion KX II-Standardport geändert werden (oder das andere Gerät muss geändert werden).

Wird die IP-Adresse des Dominion KX II geändert oder kommt ein neues Dominion KX II-Gerät hinzu, muss dem System ausreichend Zeit gegeben werden, um die IP- und MAC-Adressen in den Schicht 2- und Schicht 3-Netzwerken zu verbreiten.



IPv6-Netzwerk

Was ist IPv6?

IPv6 ist das Akronym für "Internet Protocol Version 6". IPv6 ist das IP-Protokoll der nächsten Generation, das die aktuelle Version 4 (IPv4) ersetzt.

In IPv6 werden einige Probleme von IPv4 wie die begrenzte Anzahl an IPv4-Adressen behoben. IPv4 wird so auch in einigen Bereichen wie Routing und automatische Netzwerkkonfiguration verbessert. IPv6 soll IPv4 schrittweise ersetzen, wobei beide Versionen für einige Jahre parallel existieren werden.

Durch IPv6 wird eines der größten Probleme eines IP-Netzwerks, aus Sicht des Administrators, angegangen: die Konfiguration und Verwaltung eines IP-Netzwerks.

Warum unterstützt Dominion KX II IPv6-Netzwerke?

US-Regierungsbehörden sowie das US-amerikanische Verteidigungsministerium werden demnächst IPv6-kompatible Produkte erwerben. In den nächsten Jahren werden auch viele Unternehmen und Länder wie China auf IPv6 umstellen.

Was bedeutet "Dual Stack" und warum ist diese Funktion erforderlich?

"Dual Stack" ist eine Funktion zur gleichzeitigen Unterstützung von IPv4- und IPv6-Protokollen. Durch den graduellen Übergang von IPv4 zu IPv6 ist "Dual Stack" eine grundlegende Anforderung bei der IPv6-Unterstützung.

Wie kann ich auf der Dominion KX II-Einheit IPv6 aktivieren?

Diese Einstellung können Sie über die Seite "Network Settings" (Netzwerkeinstellungen) im Menü "Device Settings" (Geräteeinstellungen) des Dominion KX II vornehmen. Aktivieren Sie die Option "IPv6 Addressing" (IPv6-Adressen verwenden) und wählen Sie die manuelle oder automatische Konfiguration aus. Sie müssen die Funktion auch im MPC aktivieren.

Was passiert, wenn ich einen externen Server mit einer IPv6-Adresse habe, den ich mit Dominion KX II verwenden möchte?

Dominion KX II kann über die IPv6-Adressen auf externe Server zugreifen (z. B. einen SNMP-Manager, Syslog-Server oder LDAP-Server).

Durch die Verwendung der Dual-Stack-Architektur des Dominion KX II kann auf diese externen Server über (1) eine IPv4-Adresse, (2) eine IPv6-Adresse oder (3) einen Hostnamen zugegriffen werden. Dominion KX II unterstützt demnach also die gemischte IPv4-/IPv6-Umgebung, über die viele Kunden verfügen.

Unterstützt Dominion KX I IPv6?

Nein, Dominion KX I unterstützt keine IPv6-Adressen.

Was passiert, wenn mein Netzwerk IPv6 nicht unterstützt?

Die Standard-Netzwerkeinstellungen des Dominion KX II sind werkseitig nur für IPv4 eingestellt. Wenn Sie IPv6 verwenden möchten, folgen Sie den oben beschriebenen Anweisungen zum Aktivieren der IPv6-/IPv4-Dual-Stack-Funktion.

Wo erhalte ich weitere Informationen zu IPv6?

Allgemeine Informationen zu IPv6 finden Sie unter www.ipv6.org. Im Benutzerhandbuch des Dominion KX II wird die Unterstützung für IPv6 des Dominion KX II erläutert.



Server

Benötigt Dominion KX II einen Windows-Server?

Auf keinen Fall. Da Sie darauf angewiesen sind, dass die KVM-Infrastruktur unter allen Umständen stets verfügbar ist (um auftretende Probleme zu lösen), wurde Dominion KX II so entwickelt, dass er vollständig unabhängig von jedem externen Server ist. Wird zum Beispiel das Rechenzentrum von einem gefährlichen Windows-Wurm oder Virus befallen, benötigen Administratoren die KVM-Lösung, um das Problem zu beheben. Daher darf die KVM-Lösung in Bezug auf die Funktion auf keinen Fall auf dieselben Windows-Server (oder irgendeinen anderen Server) angewiesen sein.

Dominion KX II ist diesbezüglich vollständig unabhängig. Selbst wenn Sie sich entscheiden, Dominion KX II zur Authentifizierung abhängig von einem Active Directory-Server zu konfigurieren, wird die eigene Authentifizierung des Dominion KX II aktiviert, sollte der Active Directory-Server nicht zur Verfügung stehen.

Muss ich einen Webserver wie Microsoft®-Internetinformationsdienste (IIS) installieren, um die Webbrowserfunktion des Dominion KX II zu nutzen?

Nein. Dominion KX II ist ein vollständig unabhängiges Gerät. Sobald der Dominion KX II-Einheit eine IP-Adresse zugewiesen wurde, ist sie mit ihren integrierten Webbrowser- und Authentifizierungsfunktionen betriebsbereit.

Welche Software muss ich installieren, um von einer bestimmten Workstation aus auf Dominion KX II zuzugreifen?

Keine. Sie können über einen Webbrowser vollständig auf Dominion KX II zugreifen. Für Modemverbindungen ist jedoch ein optional zu installierender Client erforderlich, der auf der Raritan-Website (www.raritan.com) erhältlich ist. Für Benutzer, die kein Windows-Betriebssystem verwenden, steht nun auch ein Java-basierter Client zur Verfügung.

Was muss ich tun, um einen Server für die Verbindung mit Dominion KX II vorzubereiten?

Legen Sie die Mausparameter fest, um die Maussynchronisierung bei Remoteverbindungen zu optimieren, und deaktivieren Sie die Features für die Stromzufuhrverwaltung, die sich auf die Bildschirmanzeige auswirken. Wenn Sie jedoch den neuen D2CIM-VUSB-Adapter verwenden (der den Mausmodus Absolute Mouse Synchronization™ unterstützt), müssen Sie die Mausparameter nicht manuell festlegen.

Was muss ich bei der Maussynchronisierung beachten?



Für viele KVM-über-IP-Benutzer ist die Maussynchronisierung sehr frustrierend. Die Absolute Mouse Synchronization von Dominion KX II ermöglicht eine hervorragend synchronisierte Maus, ohne dass die Mauseinstellung des Servers auf den Windows- und Apple® Mac®-Servern geändert werden muss. Für andere Server kann der Modus "Intellligent Mouse" (Intelligente Maus) oder der schnelle Ein-Cursor-Modus verwendet werden, um das Ändern der Mauseinstellungen auf dem Server zu vermeiden.

Bladeserver

Kann ich Bladeserver mit Dominion KX II verbinden?

Dies ist möglich. Dominion KX II unterstützt bekannte Bladeservermodelle der führenden Bladeserverhersteller: HP®, IBM® und Dell®.

Welche Bladeserver werden unterstützt?

Die folgenden Modelle werden unterstützt:

- Dell® PowerEdge® 1855, 1955 und M1000e
- HP BladeSystem c3000 und c7000
- IBM® BladeCenter® H und E

Hinweis: IBM BladeCenter Modelle S, T und HT verwalten Sie über die Auswahl "IBM (Other)" [IBM (Sonstige)].



Werden die Paragon-Blade-CIMs verwendet?

Nein, das Paragon II-Blade-CIM funktioniert nicht mit Dominion KX II.

Welches CIM soll ich verwenden?

Dies hängt vom Typ der KVM-Ports der jeweiligen Marke und dem Modell des verwendeten Bladeservers ab. Die folgenden CIMs werden unterstützt: DCIM-PS2, DCIM-USBG2, D2CIM-VUSB und D2CIM-DVUSB.

Welche Arten von Zugriff und Steuerung sind verfügbar?

Dominion KX II bietet automatischen & sicheren KVM-Zugriff über folgende Optionen: (1) am Serverschrank, (2) von einem Remotestandort aus über IP, (3) über das CommandCenter und (4) über Modem.

Muss ich Zugriffstasten verwenden, um zwischen Blades zu wechseln?

Bei einigen Bladeservern müssen Sie Zugriffstasten verwenden, um zwischen Blades zu wechseln. Bei Dominion KX II müssen Sie diese Zugriffstasten nicht verwenden. Klicken Sie einfach auf den Namen des Bladeservers, und Dominion KX II wechselt automatisch zum entsprechenden Blade, ohne dass Sie eine Zugriffstaste verwenden müssen.

Habe ich Zugriff auf das Verwaltungsmodul des Bladeservers?

Ja, Sie können die URL des Verwaltungsmoduls definieren, und können über Dominion KX II oder CC-SG auf dieses zugreifen. Wenn konfiguriert, können Sie mit einem Klick darauf zugreifen.

Wie viele Bladeserver kann ich mit Dominion KX II verbinden?

Aus Gründen der Leistung und Zuverlässigkeit können Sie, unabhängig vom Modell, bis zu 8 Blade-Chassis an eine Dominion KX II-Einheit anschließen. Raritan empfiehlt, bis zu doppelt so viele Remote-Verbindungen, wie sie das Gerät unterstützt, anzuschließen. Bei einem KX2-216 mit zwei Remotekanälen empfiehlt Raritan beispielsweise, bis zu 4 Bladeserver-Chassis anzuschließen. Sie können natürlich individuelle Server an die übrigen Serverports anschließen.

Ich bin ein SMB-Kunde mit einigen Dominion KX II-Geräten. Muss ich die CC-SG-Verwaltungsstation verwenden?

Nein, das müssen Sie nicht. SMB-Kunden müssen CC-SG nicht verwenden, um die neuen Bladefeatures zu nutzen.

Ich bin ein Firmenkunde und nutze CC-SG. Kann ich über CC-SG auf die Bladeserver zugreifen?

Ja. Wenn die Bladeserver auf Dominion KX II konfiguriert sind, kann der CC-SG-Benutzer über KVM-Verbindungen auf diese zugreifen. Außerdem können die Bladeserver nach Chassis oder nach benutzerdefinierten CC-SG-Ansichten gruppiert werden.

Kann In-Band- oder eingebetteter KVM-Zugriff konfiguriert werden?

Ja, In-Band- und eingebetteter Zugriff auf Bladeserver kann in CC-SG konfiguriert werden.

Auf einigen meiner Bladeserver führe ich VMWare aus. Wird dies unterstützt?

Ja, mit CC-SG können Sie virtuelle Geräte, die auf Bladeservern ausgeführt werden, anzeigen und auf diese zugreifen.

Werden virtuelle Medien unterstützt?

Virtuelle Medien werden vom D2CIM-DVUSB auf IBM BladeCenter® Modell H und E unterstützt.

Wird die absolute Maussynchronisierung unterstützt?

Server mit internen KVM-Switches innerhalb der Blade-Chassis unterstützen normalerweise keine absolute Maustechnologie. Bei HP-Bladeservern und einigen Dell-Bladeservern ist das CIM mit jedem Blade verbunden, sodass die absolute Maussynchronisierung unterstützt wird, wenn das verwendete Betriebssystem auf dem Blade diese unterstützt.

Ist der Bladezugriff sicher?

Ja, beim Bladezugriff werden alle standardmäßigen Dominion KX II-Sicherheitsfeatures wie 128-Bit- oder 256-Bit-Verschlüsselung verwendet. Außerdem sind bladespezifische Sicherheitsfeatures wie Zugriffsberechtigungen pro Blade und Zugriffstastenblockierung verfügbar, mit deren Hilfe ein unautorisierter Zugriff verhindert wird.

Unterstützt Dominion KSX II oder KX II-101 Blade Server?

Diese Produkte verfügen derzeit nicht über die neuen Bladeserverfeatures.



Installation

Was muss ich außer dem Gerät selbst zur Installation des Dominion KX II von Raritan bestellen?

Für jeden Server, den Sie an Dominion KX II anschließen möchten, benötigen Sie ein Dominion- oder Paragon-Computer Interface Module (CIM). Hierbei handelt es sich um einen direkt am Tastatur-, Video- und Mausport des Servers angeschlossenen Adapter.

Welche Art von Kabel der Kategorie 5 muss ich für meine Installation verwenden?

Für Dominion KX II kann jedes Standard-UTP-Kabel (unabgeschirmtes Twisted-Pair-Kabel) verwendet werden, egal ob Kategorie 5, 5e oder 6. In unseren Handbüchern und Marketingunterlagen ist der Einfachheit halber oftmals nur von "Cat5"-Kabeln die Rede. Tatsächlich kann jedes UTP-Kabel für Dominion KX II verwendet werden.

Welche Servertypen können mit Dominion KX II verbunden werden?

Dominion KX II ist vollständig anbieterunabhängig. Jeder Server mit standardmäßigem Tastatur-, Video- und Mausport kann angeschlossen werden.

Wie verbinde ich Server mit Dominion KX II?

Für jeden Server, den Sie an Dominion KX II anschließen möchten, benötigen Sie ein Dominion- oder Paragon-CIM, das direkt am Tastatur-, Video- und Mausport des Servers angeschlossen wird. Anschließend verbinden Sie jedes CIM mittels Standard-UTP-Kabel (Twisted-Pair) wie z. B. Kat. 5, Kat. 5e oder Kat. 6 mit Dominion KX II.

Wie weit dürfen die Server von Dominion KX II entfernt sein?

Server können im Allgemeinen abhängig vom Servertyp bis zu 45 m von Dominion KX II entfernt sein. Weitere Informationen finden Sie auf der Raritan-Website (www.raritan.com) oder unter ***Verbindungsentfernung zum Zielserver und Videoauflösung*** (auf Seite 322). Für die neuen D2CIM-VUSB- und D2CIM-DVUSB-CIMs, die virtuelle Medien und die absolute Maussynchronisierung unterstützen, wird ein Bereich von 30 m empfohlen.

Einige Betriebssysteme stürzen ab, wenn die Tastatur- oder Mausverbindung während des Betriebs getrennt wird. Wie wird der durch den Wechsel zu einem anderen Server verursachte Absturz von Dominion KX II angeschlossenen Servern verhindert?

Jeder Computer Interface Module-Kopierschutzstecker von Dominion (DCIM) fungiert als virtuelle Tastatur und Maus für den Server, an dem der Kopierschutzstecker angeschlossen ist. Hierbei spricht man von der KME-Technologie (Keyboard/Mouse Emulation, Tastatur-/Mausemulation). Die KME-Technologie von Raritan besitzt Rechenzentrumsqualität, ist ausreichend erprobt und ist weitaus zuverlässiger als die von einfacheren KVM-Switches. Diese Technologie beruht auf über 15 Jahren Erfahrung und wurde weltweit auf Millionen von Servern implementiert.

Müssen auf an Dominion KX II angeschlossenen Servern Agents installiert werden?

Die mit Dominion KX II verbundenen Server erfordern keine Installation von Softwareagents, da die Verbindung des Dominion KX II mit dem Tastatur-, Video- und Mausport des Servers direkt über Hardware hergestellt wird.

Wie viele Server können an jedes Dominion KX II-Gerät angeschlossen werden?

Die Dominion KX II-Modelle bieten 8, 16 bzw. 32 Serverports in einem 1U-Chassis oder 64 Serverports in einem 2U-Chassis. Dies ist die höchste Portdichte für digitale KVM-Switches der Branche.

Was passiert, wenn ich die Verbindung eines Servers zu Dominion KX II trenne und den Server an ein anderes Dominion KX II-Gerät oder an einen anderen Port desselben Dominion KX II-Geräts anschließe?

Dominion KX II aktualisiert automatisch die Serverportnamen, wenn Server an anderen Ports angeschlossen werden. Diese automatische Aktualisierung betrifft nicht nur den Port für den lokalen Zugriff, sondern auch alle Remoteclients und die optionale Verwaltungsanwendung CommandCenter Secure Gateway.

Wie schließe ich ein seriell gesteuertes Gerät (RS-232) wie einen Cisco-Router/-Switch oder einen Headless-Sun™-Server an Dominion KX II an?

Wenn Sie nur wenige seriell gesteuerte Geräte besitzen, können Sie diese mit dem neuen seriellen Wandler "P2CIM-SER" von Raritan an Dominion KX II anschließen.

Bei mehr als vier seriell gesteuerten Geräten empfehlen wir allerdings die Verwendung der KSX II- oder SX-Serie sicherer Konsolenserver von Raritan. Diese Geräte lassen sich einfach bedienen, konfigurieren und verwalten und können vollständig in die Implementierung einer Dominion-Serie integriert werden. Insbesondere viele UNIX- und Netzwerkadministratoren begrüßen den direkten SSH-Wechsel zu einem Gerät.



Lokaler Port

Wie kombiniere ich mehrere Dominion KX II-Geräte zu einer physischen Einzellösung?

Kann ich auf meine Server direkt über das Gestell zugreifen?

Ja. Die in einem Gestell montierte Dominion KX II-Einheit funktioniert genau wie ein herkömmlicher KVM-Switch: Sie ermöglicht die Steuerung von bis zu 64 Servern mit nur einer Tastatur, Maus und einem Monitor.

Kann ich die lokalen Ports mehrerer Dominion KX II konsolidieren?

Ja. Sie können die lokalen Ports mehrerer Dominion KX II-Switches mit einem anderen Dominion KX II verbinden, indem Sie die Schichtfunktion von Dominion KX II verwenden. Anschließend können Sie von einem einzigen Ort im Rechenzentrum mithilfe einer konsolidierten Portliste auf die mit den >ProductName<-Geräten verbundenen Server zugreifen.

Verhindere ich den Remotezugriff anderer Benutzer auf die Server, wenn ich den lokalen Port verwende?

Nein. Der lokale Dominion KX II-Port besitzt einen vollständig unabhängigen Zugriffspfad auf die Server. Dies bedeutet, ein Benutzer kann lokal über das Gestell auf die Server zugreifen, ohne die Anzahl der Benutzer einzuschränken, die gleichzeitig von einem entfernten Standort aus auf das Gestell zugreifen.

Kann ich am lokalen Port eine USB-Tastatur oder -Maus anschließen?

Ja. Dominion KX II verfügt am lokalen Port über PS/2- und USB-Tastatur-/Mausports. Die USB-Ports verwenden USB v1.1 und unterstützen nur Tastaturen und Mäuse, keine USB-Geräte wie Scanner oder Drucker.

Gibt es eine Bildschirmanzeige für den lokalen Zugriff am Serverschrank?

Ja, aber der Zugriff auf Dominion KX II am Serverschrank geht weit über konventionelle Bildschirmanzeigen hinaus. Der lokale Port des Dominion KX II bietet die erste browserbasierte Oberfläche für den lokalen und Remotezugriff auf den Serverschrank. Darüber hinaus können fast alle Verwaltungsfunktionen am Serverschrank ausgeführt werden.

Wie wähle ich zwischen Servern, während ich den lokalen Port verwende?

Der lokale Port zeigt die angeschlossenen Server über dieselbe Oberfläche an wie der Remoteclient. Durch ein einfaches Klicken stellen Sie eine Verbindung mit einem Server her.

Wie stelle ich sicher, dass nur berechtigte Benutzer über den lokalen Port auf Server zugreifen?

Für die Benutzer, die den lokalen Port verwenden möchten, gilt die gleiche Authentifizierungsebene wie für Benutzer, die von einem Remotestandort zugreifen. Dies bedeutet:

- Wenn Dominion KX II zur Interaktion mit einem externen RADIUS-, LDAP- oder Active Directory-Server konfiguriert wurde, erfolgt die Authentifizierung von Benutzern, die versuchen, auf den lokalen Port zuzugreifen, über denselben Server.
- Sind die externen Authentifizierungsserver nicht verfügbar, schaltet Dominion KX II mithilfe der Failoverfunktion auf seine eigene, interne Authentifizierungsdatenbank um.
- Dominion KX II verfügt über eine eigenständige Authentifizierung für die sofortige Installation.

Wird diese Änderung auch auf die für den Remotezugriff verwendeten Clients übertragen, wenn ich zum Ändern des Namens eines angeschlossenen Servers den lokalen Port verwende? Wird die Änderung auch von der optionalen Anwendung CommandCenter übernommen?

Ja. Der lokale Port ist mit den für den Remotezugriff verwendeten Clients und mit der optionalen Verwaltungsanwendung CommandCenter Secure Gateway von Raritan identisch und vollständig synchronisiert. Wenn Sie den Namen eines Servers über die Bildschirmanzeige des Dominion KX II ändern, werden alle Remoteclients und externen Verwaltungsserver in Echtzeit aktualisiert.

Wird die Änderung auch von der Bildschirmanzeige des lokalen Ports übernommen, wenn ich die Tools zur Remoteverwaltung des Dominion KX II zum Ändern des Namens eines angeschlossenen Servers verwende?

Ja. Wenn Sie den Namen eines Servers von einem Remotestandort aus oder mittels der optionalen Verwaltungsanwendung CommandCenter Secure Gateway von Raritan ändern, wird die Bildschirmanzeige des Dominion KX II sofort aktualisiert.

Manchmal sehe ich "Schatten" auf der Benutzeroberfläche des lokalen Ports. Wie kommt dies zustande?

Dieser Schatteneffekt tritt bei LCD-Monitoren auf, die lange Zeit eingeschaltet bleiben. Die LCD-Eigenschaften und die elektrische/statische Ladung können zu solchen Schatten führen.



Erweiterter lokaler Port (nur bei den Modellen Dominion KX2-832 und KX2-864)

Was ist der erweiterte lokale Port?

Die Modelle KX2-832 und KX2-864 verfügen über einen erweiterten lokalen Port. Die Dominion KX II-Modelle für acht Benutzer verfügen über einen lokalen Standardport und einen neuen, erweiterten lokalen Port, der den lokalen Port per Kabel der Kategorie 5 über das Gestell hinaus zu einem Kontrollraum, einer anderen Stelle im Rechenzentrum oder einem Paragon II-Switch verlängert.

Kann ich den erweiterten lokalen Port mit einem anderen Dominion KX II verbinden?

Ja, Sie können die erweiterten lokalen Ports mit einem Serverport eines anderen Dominion KX II verbinden, indem Sie die Schichtfunktion von Dominion KX II verwenden.

Ist für die Nutzung des erweiterten lokalen Ports eine User-Station erforderlich?

Ja, die folgenden Geräte können als User-Station für den erweiterten lokalen Port verwendet werden: Paragon II EUST, Paragon II UST und das Cat5 Reach URKVMG-Gerät. Zusätzlich kann der erweiterte lokale Port über ein Kabel der Kategorie 5 mit einem Serverport an einem Paragon II-Switch verbunden werden. Diese Konfiguration kann verwendet werden, um die lokalen Ports vieler KX2-8xxx-Geräte an einem einzigen Switch zusammenzufassen.

Wie weit darf die User-Station von <ProductName< entfernt sein?

Die Entfernung kann, je nach User-Station, Videoauflösung sowie Typ und Qualität des Kabels, zwischen ca. 60 und 300 m betragen.

Wird ein CIM benötigt?

Nein, es wird kein CIM benötigt? Schließen Sie einfach ein Kabel der Kategorie 5 an.

Muss ich den erweiterten lokalen Port verwenden?

Nein, der erweiterte lokale Port ist eine optionale Funktion, die standardmäßig deaktiviert ist. Auf der Seite "Local Port Settings" (Lokale Porteinstellungen) können Sie sie aktivieren. Wenn Sie den lokalen Standardport, der Ihnen zusätzliche Sicherheit bietet, nicht nutzen möchten, können Sie diesen ebenfalls deaktivieren.

Stromzufuhrsteuerung

Verfügt Dominion KX II über zwei Netzteile?

Alle Dominion KX II-Modelle verfügen über zwei Stromeingänge und Netzteile mit automatischem Failover. Sollte ein Stromeingang oder Netzteil ausfallen, wechselt Dominion KX II automatisch zum anderen.

Erkennt das Netzteil des Dominion KX II automatisch die Spannungseinstellungen?

Ja. Das Netzteil des Dominion KX II kann für einen Spannungsbereich von 100 bis 240 V bei 50 bis 60 Hz verwendet werden.

Werde ich benachrichtigt, falls ein Netzteil oder Stromeingang ausfällt?

Die LED-Anzeige an der Vorderseite des Dominion KX II zeigt einen Ausfall der Stromversorgung an. Darüber hinaus wird ein entsprechender Eintrag an das Prüfprotokoll gesendet und in der Benutzeroberfläche des Dominion KX II-Remoteclients angezeigt. Falls der Administrator dies konfiguriert hat, werden SNMP- oder Syslog-Ereignisse generiert.

Welche Funktionen zur Stromzufuhrsteuerung bietet Dominion KX II?

Die Powerstrips von Raritan zur Remote-Stromzufuhrsteuerung können an Dominion KX II angeschlossen werden, um die Stromzufuhr der KVM-Zielserver zu steuern. Sie müssen lediglich einmal einen Konfigurationsschritt ausführen und können anschließend durch Klicken mit der rechten Maustaste auf den entsprechenden Servernamen einen abgestürzten Server einschalten, ausschalten bzw. aus- und wieder einschalten. Diese Art von Neustart ist mit dem physischen Trennen des Servers vom Stromnetz und dem erneuten Anschließen vergleichbar.

Wie viele PDUs kann ich mit Dominion KX II verbinden?

An ein Dominion KX II-Gerät können bis zu acht PDUs angeschlossen werden.

Wie verbinde ich die PDU mit Dominion KX II?

Für den Anschluss eines Powerstrips am Dominion KX II-Gerät müssen Sie das CIM D2CIM-PWR verwenden. Das D2CIM-PWR muss separat erworben werden; es gehört nicht zum Lieferumfang der PDU.

Unterstützt Dominion KX II Server mit mehreren Netzteilen? Spielt es eine Rolle, wenn jedes Netzteil an einem anderen Powerstrip angeschlossen ist?



Ja. Dominion KX II kann leicht zur Unterstützung mehrerer Netzteile, die an verschiedenen Powerstrips angeschlossen sind, konfiguriert werden. An ein Dominion KX II-Gerät können bis zu acht (8) Powerstrips angeschlossen werden. Pro Zielserver können vier Netzteile mit mehreren Powerstrips verbunden werden.

Zeigt Dominion KX II Statistiken und Messungen von der PDU an?

Ja. Stromzufuhrstatistiken auf PDU-Ebene, einschließlich Stromzufuhr, Strom und Spannung, werden von der PDU abgerufen und angezeigt.

Erfordert die Remote-Stromzufuhrsteuerung eine spezielle Serverkonfiguration?

Einige Server verfügen über Standard-BIOS-Einstellungen, die beispielsweise verhindern, dass der Server nach dem Wiederherstellen der Stromzufuhr automatisch neu gestartet wird. Informationen zum Ändern dieser Einstellung finden Sie in der Dokumentation des entsprechenden Servers.

Was passiert, wenn ich einen Server aus- und wieder einschalte?

Dies ist mit dem physischen Trennen des Servers vom Stromnetz und dem erneuten Anschließen vergleichbar.

Kann ich andere an eine PDU angeschlossene Geräte (keine Server) ein-/ausschalten?

Ja. Sie können mithilfe der browserbasierten Oberfläche des Dominion KX II andere an die PDU angeschlossene Geräte nach Ausgang ein-/ausschalten.

Welche Arten von Powerstrips unterstützt Dominion KX II?

Zur Nutzung der integrierten Benutzeroberfläche für die Stromzufuhrsteuerung des Dominion KX II (und speziell für die integrierte Sicherheit) müssen Sie Raritan-Powerstrips für die Remote-Stromzufuhrsteuerung (RPC) verwenden. Diese RPCs sind in verschiedenen Buchsen-, Stecker- und Amperevariationen erhältlich. Für den Anschluss eines RPC am Dominion KX II-Gerät müssen Sie das CIM D2CIM-PWR erwerben.



Skalierbarkeit

Wie kombiniere ich mehrere Dominion KX II-Geräte zu einer physischen Einzellösung?

Um mehrere Dominion KX II-Geräte physisch zu verbinden, um einen konsolidierten lokalen Zugriff zu erhalten, können Sie die lokalen Ports mehrerer Dominion KX II-Schicht-Switches (kaskadierte Geräte) mit einem Dominion KX II-Basisgerät verbinden, dass die Schichtfunktion von Dominion KX II verwendet. Anschließend können Sie von einem einzigen Ort im Rechenzentrum mithilfe einer konsolidierten Portliste auf die mit den >ProductName<-Geräten verbundenen Server zugreifen.

Das D2CIM-DVUSB-CIM muss verwendet werden, um den Dominion KX II-Schicht-Switch mit dem Basis-Switch zu verbinden. Für KX2-832 und KX2-864 kann der erweiterte lokale Port über ein Kabel der Kategorie 5/6 (kein CIM erforderlich) mit dem Dominion KX II-Basis-Switch verbunden werden.

Der Zugriff über die konsolidierte Portliste ist im Rechenzentrum oder auch von einem Remote-PC verfügbar. Der Zugriff auf alle an das Dominion KX II-Gerät angeschlossene Server kann über eine hierarchische Portliste oder über eine Suche (mit Platzhalter) erfolgen.

Es werden zwei Ebenen von Schichten unterstützt. In einer Schichtkonfiguration kann auf maximal 1024 Geräte zugegriffen werden. Die Remote-Stromzufuhrsteuerung wird auch unterstützt.

Der Zugriff auf virtuelle Medien, Smart Cards und Blade-Server über einen Schichtzugriff wird in einer zukünftigen Version unterstützt. Diese Funktionen stehen natürlich zur Verfügung, wenn sie über eine standardmäßige Remote-Verbindung aufgerufen werden.

Der Zugriff auf den Remote-IP-Server über eine konsolidierte Portliste ist zwar praktisch, aber für eine optimale Leistung empfehlen wird den Zugriff auf den Schichtserver vom CommandCenter oder direkt über den verbundenen Dominion KX II-Server.

Muss ich die Dominion KX II-Geräte physisch miteinander verbinden?

Mehrere Dominion KX II-Einheiten müssen nicht physisch miteinander verbunden werden. Die einzelnen Dominion KX II-Einheiten werden stattdessen mit dem Netzwerk verbunden und fungieren automatisch als Einzellösung, wenn sie zusammen mit der Verwaltungsanwendung CommandCenter Secure Gateway (CC-SG) von Raritan bereitgestellt werden.

CC-SG dient als einziger Zugriffspunkt für den Remotezugriff und die Remoteverwaltung. CC-SG bietet bequeme Tools wie die gemeinsame Konfiguration, die gemeinsame Firmwareaktualisierung und eine einzelne Authentifizierung und Autorisierungsdatenbank.



Wenn Sie CC-SG für zentralisierten Remotezugriff verwenden, können Sie die Schichtfunktion (Kaskadieren) von Dominion KX II nutzen, um lokale Ports mehrerer Dominion KX II-Switches zu konsolidieren und von einer Konsole im Rechenzentrum auf maximal 1024 Server zugreifen.

Ist CC-SG erforderlich?

Wenn Sie die Standalone-Verwendung (ohne zentrales Verwaltungssystem) nutzen möchten, arbeiten mehrere Dominion KX II-Einheiten weiterhin über das IP-Netzwerk zusammen und werden automatisch skaliert. Sie können von der webbasierten Benutzeroberfläche des Dominion KX II und vom Multiplatform Client (MPC) auf mehrere Dominion KX II-Switches zugreifen.

Kann ich einen vorhandenen analogen KVM-Switch an Dominion KX II anschließen?

Ja. Analoge KVM-Switches können an einem der Dominion KX II-Serverports angeschlossen werden. Verwenden Sie einfach ein D2CIM-DVUSB oder D2CIM-VUSB, und schließen Sie es an die Benutzerports des vorhandenen analogen KVM-Switches an. Analoge KVM-Switches besitzen unterschiedliche technische Daten, und Raritan bietet keine Gewähr für die Kompatibilität analoger KVM-Switches von Drittanbietern. Weitere Informationen erhalten Sie beim technischen Kundendienst von Raritan.

Computer Interface Modules (CIMs)

Kann ich Computer Interface Modules (CIMs) vom analogen Matrix-KVM-Switch "Paragon" von Raritan mit Dominion KX II verwenden?

Ja. Bestimmte Paragon-Computer-Interface-Modules (CIMs) können mit Dominion KX II verwendet werden (eine aktuelle Liste zertifizierter CIMs finden Sie auf der Raritan-Website bei den Versionshinweisen zu Dominion KX II).

Da Paragon-CIMs jedoch teurer sind als Dominion KX II-CIMs (sie umfassen Technologie für die Videoübertragung über eine Entfernung von bis zu 300 m), sollten im Allgemeinen keine Paragon-CIMs zur Verwendung mit Dominion KX II erworben werden. Werden Paragon-CIMs an Dominion KX II angeschlossen, übertragen diese Videodaten wie Dominion KX II-CIMs über eine Entfernung von bis zu 45 m und nicht über 300 m (wie beim Anschluss an Paragon).

Kann ich die Computer Interface Modules (CIMs) des Dominion KX II mit dem analogen Matrix-KVM-Switch "Paragon" von Raritan verwenden?

Nein. Die Computer Interface Modules (CIMs) des Dominion KX II übertragen Videobilder über eine Entfernung von 15 m bis 45 m und können daher nicht mit Paragon verwendet werden, denn hierfür sind CIMs erforderlich, die Videobilder über eine Entfernung von 300 m übertragen. Um sicherzustellen, dass alle Raritan-Kunden immer die bestmögliche Videoqualität erhalten (eine typische Eigenschaft von Raritan) sind CIMs der Dominion-Serie nicht mit Paragon kompatibel.

Unterstützt Dominion KX II Paragon Dual CIMs?

Ja. Dominion KX II unterstützt auch Paragon II Dual CIMs (P2CIM-APS2DUAL und P2CIM-AUSBDUAL), die Server im Rechenzentrum mit zwei verschiedenen Dominion KX II-Switches verbinden können.

Wenn ein Dominion KX II-Switch nicht verfügbar ist, können Sie über den zweiten Dominion KX II-Switch auf den Server zugreifen. Dies ermöglicht einen redundanten Zugriff und erhöht den KVM-Remotezugriff.

Hierbei handelt es sich um Paragon-CIMs, die die erweiterten Funktionen von Dominion KX II, wie virtuelle Medien, absolute Maus usw., nicht unterstützen.



Sicherheit

Ist die Dominion KX II-Einheit FIPS 140-2-zertifiziert?

Dominion KX II ab Version 2.2.0 bietet Benutzern die Möglichkeit, ein integriertes FIPS 140-2-validiertes kryptografisches Modul zu verwenden, das gemäß der FIPS 140-2-Implementierungsanweisung auf einer Linux-Plattform ausgeführt wird. Dieses kryptografische Modul wird für die Verschlüsselung von KVM-Sitzungsdaten verwendet. Dabei handelt es sich um Video-, Tastatur-, Maus- und Smart Card-Daten sowie um die Daten von virtuellen Medien.

Welche Art von Verschlüsselung wird von Dominion KX II verwendet?

Dominion KX II verwendet sowohl für die SSL-Kommunikation als auch für den eigenen Datenstrom die standardmäßige und sehr sichere RC4- oder -AES-Verschlüsselung. Zwischen den Remoteclients und Dominion KX II werden keinerlei Daten unverschlüsselt übertragen.

Unterstützt Dominion KX II die AES-Verschlüsselung, die im Rahmen des vom US-amerikanischen National Institute of Standards and Technology entwickelten FIPS 140-2-Standards empfohlen wird?

Dominion KX II verwendet die AES (Advanced Encryption Standard)-Verschlüsselung für noch mehr Sicherheit.

Bei AES handelt es sich um einen von den US-Behörden genehmigten kryptografischen Algorithmus, der vom National Institute of Standards and Technology (NIST) in FIPS (Federal Information Processing Standard) 197 empfohlen wird.

Ermöglicht Dominion KX II die Verschlüsselung von Videodaten? Oder werden nur Tastatur- und Mausdaten verschlüsselt?

Im Gegensatz zu Konkurrenzprodukten, die nur Tastatur- und Mausdaten verschlüsseln, verschlüsselt Dominion KX II Tastatur-, Maus- und Videodaten zur Gewährleistung einer hohen Sicherheit.

Wie wird Dominion KX II in externe Authentifizierungsserver wie Active Directory®, RADIUS oder LDAP integriert?

Dominion KX II kann leicht zur Weiterleitung aller Authentifizierungsanforderungen an einen externen Server wie LDAP, Active Directory oder RADIUS konfiguriert werden. Für jeden authentifizierten Benutzer empfängt Dominion KX II die Benutzergruppe, der dieser Benutzer angehört, vom Authentifizierungsserver. Dominion KX II bestimmt daraufhin die Zugriffsrechte entsprechend der Gruppe, der der Benutzer angehört.

Wie werden Benutzernamen und Kennwörter gespeichert?



Bei der Verwendung der internen Authentifizierungsfunktionen des Dominion KX II werden alle wichtigen Informationen wie Benutzernamen und Kennwörter in einem verschlüsselten Format gespeichert. Niemand (und hierzu zählen auch der technische Kundendienst und die Entwicklungsabteilung von Raritan) kann diese Benutzernamen und Kennwörter abrufen.

Unterstützt Dominion KX II die Verwendung sicherer Kennwörter?

Der Administrator kann in Dominion KX II die Prüfung sicherer Kennwörter konfigurieren, um sicherzustellen, dass benutzerdefinierte Kennwörter unternehmensinternen Richtlinien bzw. Behördenvorschriften genügen und nicht von Hackern geknackt werden können.

Welche Verschlüsselungsebene wird erreicht, wenn der Verschlüsselungsmodus des Dominion KX II auf "Auto" (Automatisch) eingestellt ist?

Welche Verschlüsselungsebene automatisch ausgehandelt wird, hängt vom verwendeten Browser ab.

Kann ich mein eigenes digitales Zertifikat auf Dominion KX II hochladen?

Ja. Sie können selbstsignierte Zertifikate oder digitale Zertifikate einer Zertifizierungsstelle auf Dominion KX II hochladen, um die Authentifizierung und die sichere Kommunikation zu verbessern.

Unterstützt Dominion KX II eine konfigurierbare Sicherheitsmeldung?

Ja. Für Behörden, Militär und andere sicherheitsbewusste Kunden, die eine Sicherheitsmeldung vor der Benutzeranmeldung erfordern, kann Dominion KX II eine vom Benutzer konfigurierbare Sicherheitsmeldung anzeigen und optional das Akzeptieren der Bedingungen anfordern.

Meine Sicherheitsrichtlinie ermöglicht nicht die Verwendung von standardmäßigen TCP-Portnummern. Kann ich sie ändern?

Ja. Wenn Sie die standardmäßigen TCP/IP-Portnummern vermeiden möchten, um die Sicherheit zu erhöhen, ermöglicht Dominion KX II dem Administrator die Konfiguration alternativer Portnummern.



Smart Card- und CAC-Authentifizierung

Unterstützt <ProductName< die Smart Card- und CAC-Authentifizierung?

Ja, Smart Card- und DoD Common Access Card (CAC)-Authentifikation an Zielservern wird ab Version 2.1.10 unterstützt.

Welche <ProductName<-Modelle unterstützen Smart Cards/CAC?

Alle Dominion KX II-Modelle unterstützen Smart Cards/CAC. Die Modelle Dominion KSX2 und KX2-101 unterstützen derzeit noch keine Smart Cards und CAC.

Verwenden Unternehmens- und SMB-Kunden auch Smart Cards?

Ja. Die Bundesregierung der USA weist den intensivsten Einsatz von Smart Cards auf.

Welche CIMs unterstützen Smart Cards/CAC?

Es wird ein D2CIM-DVUSB benötigt. Dieses CIM muss auf die Firmwareversion 2.1.10 und höher aktualisiert sein.

Welche Firmwareversion wird benötigt?

Es wird die Dominion KX II-Version 2.1.10 und höher benötigt.

Welche Smart Card-Lesegeräte werden unterstützt?

Die unterstützten Standards bei Lesegeräten sind USB CCID und PC/SC. Eine Liste der zugelassenen Lesegeräte und weitere Informationen finden Sie unter Dominion KX II 2.1.10 ***Unterstützte und nicht unterstützte Smart Card-Lesegeräte*** (auf Seite 326) oder in den Versionshinweisen.

Funktioniert die Smart Card-/CAC-Authentifizierung am lokalen Port und über Command Center?

Ja. Schließen Sie ein kompatibles Smart Card-Lesegerät an den USB-Port von Dominion KX II an.

Werden die Smart Card-aktivierte UST und das CIM von Paragon verwendet?

Nein, die P2-EUST/C und das P2CIM-AUSB-C gehören nicht zur Dominion KX II-Lösung.

Bedienkomfort

Kann Dominion KX II von einem Remotestandort aus über einen Webbrowser verwaltet und konfiguriert werden?

Ja, Dominion KX II kann von einem Remotestandort aus vollständig über einen Webbrowser konfiguriert werden. Hierzu muss auf Ihrer Workstation jedoch die entsprechende Version der Java Runtime Environment (JRE) installiert sein.

Außer der anfänglichen Einstellung der IP-Adresse des Dominion KX II können alle Lösungsparameter vollständig über das Netzwerk eingerichtet werden. (Über ein Ethernet-Crossoverkabel und die Dominion KX II-Standard-IP-Adresse können Sie sogar die Ersteinstellungen über einen Webbrowser konfigurieren.)

Kann ich die Dominion KX II-Konfiguration sichern und wiederherstellen?

Ja, die Dominion KX II-Konfigurationen für Benutzer und Geräte können zur späteren Wiederherstellung (z. B. nach einer Katastrophe) vollständig gesichert werden.

Die Funktionen zur Sicherung und Wiederherstellung des Dominion KX II können von einem Remotestandort über das Netzwerk bzw. über die Remotekonsole genutzt werden.

Welche Prüfungs- oder Protokollierungsarten bietet Dominion KX II?

Zur besseren Nachprüfung protokolliert Dominion KX II alle wichtigen Benutzer- und Systemereignisse mit einem Datums- und Zeitstempel. Zu den protokollierten Ereignissen zählen u. a.: die Benutzeran- und -abmeldung, der Benutzerzugriff auf einen bestimmten Server, fehlgeschlagene Anmeldeversuche, Konfigurationsänderungen usw.

Kann Dominion KX II in Syslog integriert werden?

Ja. Dominion KX II besitzt nicht nur eigene interne Protokollfunktionen, Dominion KX II kann auch alle protokollierten Ereignisse an einen zentralen Syslog-Server senden.

Kann Dominion KX II in SNMP integriert werden?

Ja. Dominion KX II besitzt nicht nur eigene interne Protokollfunktionen, Dominion KX II kann auch SNMP-Traps an SNMP-Verwaltungssysteme wie HP Openview und CC-NOC von Raritan senden.

Kann die interne Uhr des Dominion KX II mit einem Zeitserver synchronisiert werden?



Ja, Dominion KX II unterstützt das Standard-NTP-Protokoll für die Synchronisierung mit einem Firmenzeitserver oder mit einem öffentlichen Zeitserver (vorausgesetzt, ausgehende NTP-Anforderungen können über die Firmenfirewall übertragen werden).

Verschiedenes

Wie lautet die Standard-IP-Adresse des Dominion KX II?

192.168.0.192

Wie lautet der Standardbenutzername und das Standardkennwort des Dominion KX II?

Der Standardbenutzername des Dominion KX II lautet "admin", das Standardkennwort "raritan" (alle kleingeschrieben). Für eine höchstmögliche Sicherheit wird der Administrator des Dominion KX II jedoch beim ersten Hochfahren der Dominion KX II-Einheit gezwungen, diese Standardeinstellungen zu ändern.

Ich habe mein Dominion KX II-Administratorkennwort geändert und vergessen. Kann mir Raritan helfen, das Kennwort abzurufen?

Dominion KX II verfügt über eine Taste zum Zurücksetzen, mit der das Gerät auf die Werkseinstellungen zurückgesetzt werden kann. Dadurch wird auch das Administratorkennwort zurückgesetzt.

Ich habe mich über Firefox® bei Dominion KX II angemeldet und anschließend ein weiteres Firefox-Fenster geöffnet. In diesem zweiten Firefox-Browserfenster werde ich automatisch am gleichen Dominion KX II angemeldet. Ist das korrekt?

Ja, diese Verhaltensweise ist korrekt und entspricht der Funktionsweise von Browsern und Cookies.

Wenn ich mich über Firefox bei Dominion KX II und über einen weiteren Firefox-Browser auf einem anderen Dominion KX II anmelde, werde ich von beiden Dominion KX II abgemeldet. Ist dieses Verhalten korrekt?

Ja, für den Zugriff auf zwei verschiedene Dominion KX II-Geräte müssen Sie entweder die erste Sitzung beenden oder einen anderen Client-PC verwenden.

Der Firefox-Browser scheint blockiert zu sein, wenn bestimmte Dialogfelder im Virtual KVM Client geöffnet werden. Was kann ich tun?

Dieses Verhalten ist normal, da bei Firefox alle Sitzungen miteinander verbunden sind. Wenn Sie das Dialogfeld des Virtual KVM Client schließen, wird Firefox nicht mehr blockiert.

Index

A

B

C



D

E

F

G



H

I

J

K

L

M

N



O

P

R

S



T

U

V



W

Z





USA/Kanada/Lateinamerika

Montag bis Freitag
08:00 bis 20:00 Uhr ET (Eastern Time)
Tel.: 800-724-8090 oder 732-764-8886
CommandCenter NOC: Drücken Sie auf Ihrem Telefon die Zifferntaste 6 und dann die Zifferntaste 1.
CommandCenter Secure Gateway: Drücken Sie auf Ihrem Telefon die Zifferntaste 6 und dann die Zifferntaste 2.
Fax: 732-764-8887
E-Mail-Adresse für CommandCenter NOC: tech-ccnoc@raritan.com
E-Mail-Adresse für alle anderen Produkte: tech@raritan.com

China

Peking

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +86-10-88091890

Shanghai

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +86-21-5425-2499

GuangZhou

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +86-20-8755-5561

Indien

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +91-124-410-7881

Japan

Montag bis Freitag
09:30 bis 17:30 Uhr Ortszeit
Tel.: +81-3-3523-5991
E-Mail: support.japan@raritan.com

Europa

Europa

Montag bis Freitag
08:30 bis 17:00 Uhr GMT+1 MEZ
Tel.: +31-10-2844040
E-Mail: tech.europe@raritan.com

Großbritannien

Montag bis Freitag
08:30 bis 17:00 Uhr GMT
Telefon +44(0)20-7090-1390

Frankreich

Montag bis Freitag
08:30 bis 17:00 Uhr GMT+1 MEZ
Tel.: +33-1-47-56-20-39

Deutschland

Montag bis Freitag
08:30 bis 17:30 Uhr GMT+1 MEZ
Tel.: +49-20-17-47-98-0
E-Mail: rg-support@raritan.com

Melbourne, Australien

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +61-3-9866-6887

Taiwan

Montag bis Freitag
09:00 bis 18:00 Uhr GMT -5 Standardzeit -4 Sommerzeit
Tel.: +886-2-8919-1333
E-Mail: support.apac@raritan.com